Leandro Vendramin

Non-commutative algebra

Notes

Saturday 26th March, 2022

Preface

The notes correspond to the master course *Non-commutative Algebra* of the Vrije Universiteit Brussel, Faculty of Sciences, Department of Mathematics and Data Sciences. The course is divided into thirteen two-hours lectures.

Most of the material is based on standard results on group algebras covered in the VUB course *Associative Algebras*. Lecture notes for this course are freely available at `https://github.com/vendramin/associative`. Basic texts on group algebras are Lam's book [11] and Passman's book [12].

This version was compiled on Saturday 26$^{\text{th}}$ March, 2022 at 16:03.

Leandro Vendramin
Brussels, Belgium

Contents

List of topics

Lecture 1

§1. Group rings

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

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

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

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

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

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

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

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

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

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

and multiplication

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

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

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

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

Despite the fact that there are several cases were the isomorphism problem has an affirmative answer (e.g. abelian groups, metabelian groups, nilpotent groups, nilpotent-by-abelian groups, simple groups, abelian-by-nilpotent groups), it is false in general. In 2001 Hertweck found a counterexample of order $2^{21}97^{28}$, see [7].

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

Question 1.2 has an affirmative answer in several cases. However, it is not true in general. This question recently answered by García, Margolis and del Río [4]. They found two non-isomorphic groups G and H both of order 512 such that $K[G]\simeq K[H]$ for all field K of characteristic two.

§2. Kapanskly's problems

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

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

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

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

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

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

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

prob:dominio **Open problem 2.1 (Zero divisors).** Let G be a torsion-free group. Is it true that $K[G]$ is a domain?

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

prob:units

Open problem 2.2 (Units). Let G be a torsion-free group. Is it true that all units of $K[G]$ are trivial?

The unit problem is still open for fields of characteristic zero. However, it was recently solved by Gardam [5] in the case of K the field of two elements. We will present Gardam's theorem as a computer calculation. We will use GAP [3].

Lemma 2.4. *The group* $G = \langle a, b : a^{-1}b^2a = b^{-2}, b^{-1}a^2b = a^{-2}\rangle$ *is torsion-free. Moreover, the subgroup* $N = \langle a^2, b^2, (ab)^2\rangle$ *is normal in* G*, free-abelian of rank three and* $G/N \simeq C_2 \times C_2$.

Proof. We first construct the group.

```
gap> F := FreeGroup(2);;
gap> A := F.1;;
gap> B := F.2;;
gap> rels := [(B^2)^A*B^2,(A^2)^B*A^2];;
gap> G := F/rels;;
gap> a := G.1;;
gap> b := G.2;;
```

Now we construct the subgroup N generated by a^2, b^2 and $(ab)^2$. It is easy to check that N is normal in G and that $G/N \simeq C_2 \times C_2$. It is even easier to do this with the computer.

```
gap> N := Subgroup(G, [a^2,b^2,(a*b)^2]);;
gap> IsNormal(G,N);
true
gap> StructureDescription(G/N);
"C2 x C2"
```

It is easy to check by hand that N is abelian, and not so easy to do it with the computer. For example,

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

We use the computer to show that N is free abelian of rank three.

```
gap> AbelianInvariants(N);
[ 0, 0, 0 ]
```

Let us prove that G is torsion-free. Let $x = a^2$, $y = b^2$ and $z = (ab)^2$. Since $(G : N) = 4$, the group G decomposes as a disjoint union $G = N \cup aN \cup bN \cup (ab)N$. Let $g \in G$ be a non-trivial element of finite order. Since N is torsion-free, $g \in aN \cup bN \cup (ab)N$. Without loss of generality we may assume that $g \in aN$, so $g = an$ for some $n \in N$. Let $\pi\colon G \to G/N$ be the canonical map. Since $g \notin N$ and $\pi(g) \in G/N \simeq C_2 \times C_2$,

$$\pi(g^2) = \pi(g)^2 = 1$$

so $g^2 \in N$ and hence $g^2 = 1$, as N is torsion-free. Thus

$$1 = g^2 = (an)^2 = (an)(an) = a^2(a^{-1}na)n = x(a^{-1}na)n.$$

Write $n = x^i y^j z^k$ for some $i, j, k \in \mathbb{Z}$. Then

$$a^{-1}na = (a^{-1}x^i a)(a^{-1}y^j a)(a^{-1}z^k a) = x^i t^{-j} z^{-k}$$

and hence $(a^{-1}na)n = x^{2i}$. Then it follows that $1 = g^2 = x(a^{-1}na)n = x^{2i+1}$, a contradiction. □

Let P be the group generated by

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

The group P appears in the literature with various names. For us P will be the Promislow group. It is easy to check that there exists a surjective group homomorphism $G \to P$. Prove that $G \simeq P$.

thm:Gardam

Theorem 2.5 (Gardam). *Let $\mathbb{F}_2$ be the field of two elements. Consider the elements $x = a^2$, $y = b^2$ and $z = (ab)^2$ of P and let*

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

Then $u = p + qa + rb + sab$ is a non-trivial unit in $\mathbb{F}_2[P]$.

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

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

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

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

Now we create the group algebra $F[P]$ and the embedding $P \hookrightarrow F[P]$. The field $\mathbb{F}_2$ will be `GF(2)` and the embedding will be denoted by `f`.

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

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

```
gap> x := Image(f, a^2);;
```

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

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

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

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

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

Now it is time to prove the theorem.

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

This completes the proof of the theorem. □

Our proof of Theorem 2.5 is exactly as that of [5].

Exercise 2.6. Let p be a prime number and $\mathbb{F}_p$ be the field of size p. Use the technique for proving Gardam's theorem to prove Murray's theorem on the existence on non-trivial units in $\mathbb{F}_p[P]$. Reference: arXiv:2106.02147.

Lecture 2

We now describe some very-well known open problems in the theory of group rings and the connection between them.

Definition 2.7. A ring R is **reduced** if for all $r \in R$ such that $r^2 = 0$ one has $r = 0$.

Integral domains and boolean rings are reduced. $\mathbb{Z}/8$ and $M_2(\mathbb{R})$ are not reduced.

Example 2.8. $\mathbb{Z}^n$ with $(a_1, \dots, a_n)(b_1, \dots, b_n) = (a_1 b_1, \dots, a_n b_n)$ is reduced.

The structure of reduced rings is described by Andrunakevic–Rjabuhin's theorem. It states that a ring is reduced if and only if it is a subdirect products of domains. See [6, 3.20.5] for a proof.

prob:reducido **Open problem 2.3.** Let G be a torsion-free group. Is it true that $K[G]$ is reduced?

Recall that if R is a unitary ring, one proves that the Jacobson radical $J(R)$ is the set of elements x such that $1 + \sum_{i=1}^{n} r_i x s_i$ is invertible for all n and all $r_i, s_i \in R$.

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

Recall that an element e of a ring is said to be *idempotent* if $e^2 = e$. Examples of idempotents are 0 and 1 and these are known as the trivial idempotents.

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

Exercise 2.9. Prove that if $K[G]$ has no zero-divisors and $\alpha \in K[G]$ is an idempotent, then $\alpha \in \{0, 1\}$.

Exercise 2.10. Prove that $K[C_4]$ contains non-trivial zero divisors and every idempotent of $K[C_4]$ is trivial.

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

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

We first prove that an affirmative solution to the Units Problem 2.2 yields a solution to Problem 2.3 about the reducibility of group algebras.

Theorem 2.11. *Let K be a field of characteristic $\neq 2$ and G be a non-trivial group. Assume that $K[G]$ has only trivial units. Then $K[G]$ is reduced.*

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

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

it follows that $1-\alpha$ is a unit of $K[G]$. Since units of $K[G]$ are trivial, there exist $\lambda \in K \setminus \{0\}$ and $g \in G$ such that $1-\alpha = \lambda g$. We claim that $g = 1$. If not,

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

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

Exercise 2.12. What happens if K is a field of characteristic two?

We now prove that an affirmative solution to the Units Problem 2.2 also yields a solution to the Jacobson Semisimplicity Problem 2.4.

Theorem 2.13. *Let G be a non-trivial group. Assume that $K[G]$ has only trivial units. If $|K| > 2$ or $|G| > 2$, then $J(K[G]) = \{0\}$.*

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

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

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

Exercise 2.14. Prove that if $G = \langle g \rangle \simeq \mathbb{Z}/2$, then $J(\mathbb{F}_2[G]) = \{0, g-1\} \neq \{0\}$.

§3. The transfer map

Now we prove that an affirmative solution to the Units Problem (Open Problem 2.2) yields a solution to Open Problem 2.1 about zero divisors in group algebras. The proof is hard and requires some preliminaries. We first need to discuss a group theoretical tool known as the *transfer map*.

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

lem:d **Lemma 3.1.** *Let G be a group and H be a subgroup of G of finite index. Let R and S be transversals of H in G and let $\alpha\colon H \to H/[H,H]$ be the canonical map. Then*

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

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

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

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

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

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

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

We are know ready to state and prove the theorem:

thm:transfer **Theorem 3.2.** *Let G be a group and H be a finite-index subgroup of G. The map*

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

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

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

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

The theorem justifies the following definition:

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

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

of Theorem 3.2, where R is some transversal of H in G.

We need methods for computing the transfer map. If H is a subgroup of G and $(G:H) = n$, let $T = \{x_1,\dots,x_n\}$ be a transversal of H. For $g \in G$ let

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

where the product is taken over all pairs $(x,y)\in(Tg)\times T$ such that $Hx=Hy$ and $\alpha\colon H\to H/[H,H]$ is the canonical map. If we write $x=x_ig$ for some $i\in\{1,\dots,n\}$, then $Hx_ig=Hx_{\sigma(i)}$ for some permutation $\sigma\in\mathbb{S}_n$. Thus

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

The cycle structure of σ turns out to be important. For example, if $\sigma=(12)(345)$ and $n=5$, then a direct calculation shows that

$$\prod_{i=1}^{5}\alpha\left(x_igx_{\sigma(i)}^{-1}\right)=\alpha(x_1g^2x_1^{-1})\alpha(x_3g^3x_3^{-1}).$$

This is precisely the content of the following lemma.

lem:transfer

Lemma 3.4. *Let G be a group and H be a subgroup of index n. Let $T=\{t_1,\dots,t_n\}$ be a transversal of H in G. For each $g\in G$ there exist $m\in\mathbb{Z}_{>0}$ and elements $s_1,\dots,s_m\in T$ and positive integers $n_1,\dots,n_m$ such that $s_i^{-1}g^{n_i}s_i\in H$, $n_1+\cdots+n_m=n$ and*

$$\nu(g)=\prod_{i=1}^{m}\alpha(s_i^{-1}g^{n_i}s_i).$$

Proof. For each i there exist $h_1,\dots,h_n\in H$ and $\sigma\in\mathbb{S}_n$ such that $gt_i=t_{\sigma(i)}h_i$. Write σ as a product of disjoint cycles, say

$$\sigma=\alpha_1\cdots\alpha_m.$$

Let $i\in\{1,\dots,n\}$ and write $\alpha_i=(j_1\cdots j_{n_i})$. Since

$$gt_{j_k}=t_{\sigma(j_k)}h_{j_k}=\begin{cases}t_{j_1}h_{j_k} & \text{si } k=n_i,\\ t_{j_{k+1}}h_{j_k} & \text{otherwise,}\end{cases}$$

then

$$\begin{aligned}
t_{j_1}^{-1}g^{n_i}t_{j_1}&=t_{j_1}^{-1}g^{n_i-1}gt_{j_1}\\
&=t_{j_1}^{-1}g^{n_i-1}t_{j_2}h_{j_1}\\
&=t_{j_1}^{-1}g^{n_i-2}gt_{j_2}h_{j_1}\\
&=t_{j_1}^{-1}g^{n_i-2}t_{j_3}h_{j_2}h_{j_1}\\
&\ \ \vdots\\
&=t_{j_1}^{-1}gt_{j_{n_i}}h_{n_{i-1}}\cdots h_{j_2}h_{j_1}\\
&=t_{j_1}^{-1}t_{j_1}h_{j_{n_i}}\cdots h_{j_2}h_{j_1}\in H.
\end{aligned}$$

Thus $s_i=t_{j_1}\in T$. It only remains to note that $\nu(g)=h_1\cdots h_n$. $\square$

An application:

pro:center **Proposition 3.5.** *If G is a group such that $Z(G)$ has finite index n, then $(gh)^n = g^n h^n$ for all $g, h \in G$.*

Proof. Note that we may assume that $\alpha = \mathrm{id}$, as $Z(G)$ is abelian. Let $g \in G$. By Lemma 3.4 there are positive integers $n_1, \dots, n_k$ such that $n_1 + \cdots + n_k = n$ and elements $t_1, \dots, t_k$ of a transversal of $Z(G)$ in G such that

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

Since $g^{n_i} \in Z(G)$ for all $i \in \{1, \dots, k\}$ (as $t_i g^{n_i} t_i^{-1} \in Z(G)$), it follows that

$$\nu(g) = g^{n_1 + \cdots + n_k} = g^n.$$

Now Theorem 3.2 implies the claim. □

The same idea implies the following property:

xca:K_central **Exercise 3.6.** If G is a group and K is a central subgroup of finite index n, then $(gh)^n = g^n h^n$ for all $g, h \in G$.

For a group G we consider

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

Exercise 3.7. Prove that $\Delta(\Delta(G)) = \Delta(G)$.

A subgroup H of G is a **characteristic** subgroup of G if $f(H) \subseteq H$ for all $f \in \mathrm{Aut}(G)$. The center and the commutator subgroup of a group are characteristic subgroups. Every characteristic subgroup is a normal subgroup.

Exercise 3.8. Prove that if H is characteristic in K and K is normal in G, then H is normal in G.

Proposition 3.9. *If G is a group, then $\Delta(G)$ is a characteristic subgroup of G.*

Proof. We first prove that $\Delta(G)$ is a subgroup of G. If $x, y \in \Delta(G)$ and $g \in G$, then $g(xy^{-1})g^{-1} = (gxg^{-1})(gyg^{-1})^{-1}$. Moreover, $1 \in \Delta(G)$. Let us show now that $\Delta(G)$ is characteristic in G. If $f \in \mathrm{Aut}(G)$ and $x \in G$, then, since

$$f(gxg^{-1}) = f(g)f(x)f(g)^{-1},$$

it follows that $f(x) \in \Delta(G)$. □

Exercise 3.10. Prove that if $G = \langle r, s : s^2 = 1, srs = r^{-1} \rangle$ is the infinite dihedral group, then $\Delta(G) = \langle r \rangle$.

Exercise 3.11. Let H and K be finite-index subgroups of G. Prove that

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

Lecture 3

§4. Passman's theorem

pro:FCabeliano

Proposition 4.1. *If G is a torsion-free group such that $\Delta(G) = G$, then G is abelian.*

Proof. Let $x, y \in G = \Delta(G)$ and $S = \langle x, y\rangle$. The group $Z(S) = C_S(x) \cap C_S(y)$ has finite index, say n, in S. By Proposition 3.5, the map $S \to Z(S)$, $s \mapsto s^n$, is a group homomorphism. Thus

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

as $x^n \in Z(S)$. Since G is torsion-free, $[x, y] = 1$. $\square$

lem:Neumann

Lemma 4.2 (Neumann). *Let $H_1, \dots, H_m$ be subgroups of G. Assume there are finitely many elements $a_{ij} \in G$, $1 \le i \le m$, $1 \le j \le n$, such that*

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

Then some H_i has finite index in G.

Proof. We proceed by induction on m. The case $m = 1$ is trivial. Let us assume that $m \ge 2$. If $(G : H_1) = \infty$, there exists $b \in G$ such that

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

Since $H_1 b \subseteq \bigcup_{i=2}^{m} \bigcup_{j=1}^{n} H_i a_{ij}$, it follows that

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

Hence G can be covered by finitely many cosets of $H_2,\dots,H_m$. By the inductive hypothesis, some of these H_j has finite index in G. $\square$

We now consider a projection operator of group algebras. If G is a group and H is a subgroup of G, let

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

If R and S are rings, a (R,S)-bimodule is an abelian group M that is both a left R-module and a right S-module and the compatibility condition

$$(rm)s=r(ms)$$

holds for all $r\in R$, $s\in S$ and $m\in M$.

Exercise 4.3. Let G be a group and H be a subgroup of G. Prove that if $\alpha\in K[G]$, then π_H is a $(K[H],K[H])$-bimodule homomorphism with usual left and right multiplications,

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

for all $\beta,\gamma\in K[H]$.

lem:escritura

Lemma 4.4. *Let X be a left transversal of H in G. Every $\alpha\in K[G]$ can be written uniquely as*

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

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

Proof. Let $\alpha\in K[G]$. Since $\operatorname{supp}\alpha$ is finite, $\operatorname{supp}\alpha$ is contained in finitely many cosets of H, say $x_1H,\dots,x_nH$, where each x_j belongs to X. Write $\alpha=\alpha_1+\cdots+\alpha_n$, where $\alpha_i=\sum_{g\in x_iH}\lambda_g g$. If $g\in x_iH$, then $x_i^{-1}g\in H$ and hence

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

with $\alpha_x\in K[H]$ for all $x\in X$. For the uniqueness, note that for each $x\in X$ the previous exercise implies that

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

as

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

$\square$

lem:ideal_pi

Lemma 4.5. *Let G be a group and H be a subgroup of G. If I is a non-zero left ideal of $K[G]$, then $\pi_H(I) \neq \{0\}$.*

Proof. Let X be a left transversal of H in G and $\alpha \in I \setminus \{0\}$. By Lemma 4.4 we can write $\alpha = \sum_{x\in X} x\alpha_x$ with $\alpha_x = \pi_H(x^{-1}\alpha) \in K[H]$ for all $x \in X$. Since $\alpha \neq 0$, there exists $y \in X$ such that $0 \neq \alpha_y = \pi_H(y^{-1}\alpha) \in \pi_H(I)$ ($y^{-1}\alpha \in I$ since I is a left ideal). □

Another application:

Proposition 4.6. *Let G be a group, H be a subgroup of G and $\alpha \in K[H]$. The following statements hold:*

1) *α is invertible in $K[H]$ if and only if α is invertible in $K[G]$.*
2) *α is a zero divisor of $K[H]$ if and only if α is a zero divisor of $K[G]$.*

Proof. If α is invertible in $K[G]$, there exists $\beta \in K[G]$ such that $\alpha\beta = \beta\alpha = 1$. Apply π_H and use that π_H is a $(K[H], K[H])$-bimodule homomorphism to obtain

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

Assume now that $\alpha\beta = 0$ for some $\beta \in K[G] \setminus \{0\}$. Let $g \in G$ be such that $1 \in \operatorname{supp}(\beta g)$. Since $\alpha(\beta g) = 0$,

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

where $\pi_H(\beta g) \in K[H] \setminus \{0\}$, as $1 \in \operatorname{supp}(\beta g)$. □

lem:Passman

Lemma 4.7 (Passman). *Let G be a group and $\gamma_1, \gamma_2 \in K[G]$ be such that $\gamma_1 K[G]\gamma_2 = \{0\}$. Then $\pi_{\Delta(G)}(\gamma_1)\pi_{\Delta(G)}(\gamma_2) = \{0\}$.*

Proof. It is enough to show that $\pi_{\Delta(G)}(\gamma_1)\gamma_2 = \{0\}$, as in this case

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

Write $\gamma_1 = \alpha_1 + \beta_1$, where

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

The subgroup $C = \bigcap_{i=1}^r C_G(u_i)$ has finite index in G. Assume that

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

Let $g \in \operatorname{supp}(\alpha_1\gamma_2)$. If v_i is a conjugate in G of some gw_j^{-1}, let $g_{ij} \in G$ be such that $g_{ij}^{-1}v_ig_{ij} = gw_j^{-1}$. If v_i and gw_j^{-1} are not conjugate, we take $g_{ij} = 1$.

For every $x \in C$ it follows that $\alpha_1\gamma_2 = (x^{-1}\alpha_1x)\gamma_2$. Since

$$x^{-1}\gamma_1 x\gamma_2 \in x^{-1}\gamma_1 K[G]\gamma_2 = 0,$$

it follows that

$$\begin{aligned}(a_1u_1+\cdots+a_ru_r)\gamma_2 &= \alpha_1\gamma_2 = x^{-1}\alpha_1 x\gamma_2 = -x^{-1}\beta_1 x\gamma_2\\ &= -x^{-1}(b_1v_1+\cdots+b_sv_r)x(c_1w_1+\cdots+c_tw_t).\end{aligned}$$

Now $g\in\operatorname{supp}(\alpha_1\gamma_2)$ implies that there exist i,j such that $g=x^{-1}v_ixw_j$. Thus v_i and gw_j^{-1} are conjugate and hence $x^{-1}v_ix=gw_j^{-1}=g_{ij}^{-1}v_ig_{ij}$, that is $x\in C_G(v_i)g_{ij}$. This proves that

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

Since C has finite index in G, it follows that G can be covered by finitely many cosets of the $C_G(v_i)$. Every $v_i\notin\Delta(G)$, so each $C_G(v_i)$ has infinite index in G, a contradiction to Neumann's lemma. □

Before proving Passman's theorem, we need to mention that if G is a torsion-free abelian group, then $K[G]$ has no non-zero divisors. We will prove this fact later, as an application of the theory of bi-ordered groups (see Corollary 6.15).

thm:Passman

Theorem 4.8 (Passman). *Let G be a torsion-free group. If $K[G]$ is reduced, then $K[G]$ is a domain.*

Proof. Assume that $K[G]$ is not a domain. Let $\gamma_1,\gamma_2\in K[G]\setminus\{0\}$ be such that $\gamma_2\gamma_1=0$. If $\alpha\in K[G]$, then

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

and thus $\gamma_1\alpha\gamma_2=0$, as $K[G]$ is reduced. In particular, $\gamma_1K[G]\gamma_2=\{0\}$. Let I be the left ideal of $K[G]$ generated by γ_2. Since $I\neq\{0\}$, it follows from Lemma 4.5 that $\pi_{\Delta(G)}(I)\neq\{0\}$. Hence $\pi_{\Delta(G)}(\beta\gamma_2)\neq\{0\}$ for some $\beta\in K[G]$. Similarly, $\pi_{\Delta(G)}(\gamma_1\alpha)\neq\{0\}$ for some $\alpha\in K[G]$. Since

$$\gamma_1\alpha K[G]\beta\gamma_2\subseteq\gamma_1K[G]\gamma_2=\{0\},$$

it follows that $\pi_{\Delta(G)}(\gamma_1\alpha)\pi_{\Delta(G)}(\beta\gamma_2)=\{0\}$ by Passman's lemma. Hence $K[\Delta(G)]$ has zero divisors, a contradictions since $\Delta(G)$ is an abelian group. □

Lecture 4

§5. More applications of the transfer

Let us start with a group-theoretic application of the transfer map. We start with some applications to the theory of finite groups.

prop:semidirecto

Proposition 5.1. *Let G be a finite group and H a central subgroup of index n, where n is coprime with $|H|$. Then $G \simeq N \rtimes H$.*

Proof. Since H is abelian, $H = H/[H,H]$. Let $\nu\colon G \to H$ be the transfer map and $h \in H$. By Lemma 3.4,

$$\nu(h) = \prod_{i=1}^{m} s_i^{-1} h^{n_i} s_i,$$

where each $s_i^{-1} h^{n_i} s_i \in H$. Since $h^{n_i} \in H \subseteq Z(G)$ for all i, it follows that $s_i^{-1} h^{n_i} s_i = h^{n_i}$ for all i. Thus

$$\nu(h) = \prod_{i=1}^{m} s_i^{-1} h^{n_i} s_i = \prod_{i=1}^{m} h^{n_i} = h^{\sum_{i=1}^{m} n_i} = h^n.$$

The composition $f\colon H \hookrightarrow G \xrightarrow{\nu} H$ is a group homomorphism. We claim that it is an isomorphism. It is injective: If $h^n = 1$, then $|h|$ divides both $|H|$ and n. Since n and $|H|$ are coprime, $h = 1$. It is surjectice: Since n and $|H|$ are coprime, there exists $m \in \mathbb{Z}$ such that $nm \equiv 1 \bmod |H|$. If $h \in H$, then $h^m \in H$ and $\nu(h^m) = h^{nm} = h$.

Let $N = \ker f$. We claim that $G = N \rtimes H$. By definition, N is normal in G and $N \cap H = \{1\}$. To show that $G = NH$ note that $|NH| = |N||H|$ and $G/N \simeq H$. □

Exercise 5.2. Let H be a central subgroup of a finite group G. If $|H|$ and $|G/H|$ are coprime, then $G \simeq H \times G/H$.

An application to infinite groups taken from Serre's book [13, 7.12].

Theorem 5.3. *Let G be a torsion-free group that contains a finite-index subgroup isomorphic to $\mathbb{Z}$. Then $G \simeq \mathbb{Z}$.*

Proof. We may assume that G contains a finite-index normal subgroup isomorphic to $\mathbb{Z}$. Indeed, if H is a finite-index subgroup of G such that $H \simeq \mathbb{Z}$, then $K = \cap_{x \in G} xHx^{-1}$ is a non-trivial normal subgroup of G (because $K = \mathrm{Core}_G(H)$ and G has no torsion) and hence $K \simeq \mathbb{Z}$ (because $K \subseteq H$) and $(G:K) = (G:H)(H:K)$ is finite. The action of G on K by conjugation induces a group homomorphism $\epsilon\colon G \to \mathrm{Aut}(K)$. Since $\mathrm{Aut}(K) \simeq \mathrm{Aut}(\mathbb{Z}) = \{-1, 1\}$, there are two cases to consider.

Assume first that $\epsilon = \mathrm{id}$. Since $K \subseteq Z(G)$, let $\nu\colon G \to K$ be the transfer homomorphism. By Proposition 3.5 (more precisely, by Exercise 3.6), $\nu(g) = g^n$, where $n = (G:K)$. Since G has no torsion, ν is injective. Thus $G \simeq \mathbb{Z}$ because it is isomorphic to a subgroup of K.

Assume now that $\epsilon \neq \mathrm{id}$. Let $N = \ker \epsilon \neq G$. Since $K \simeq \mathbb{Z}$ is abelian, $K \subseteq N$. The result proved in the previous paragraph applied to $\epsilon|_N = 1$ implies that $N \simeq \mathbb{Z}$, as N contains a finite-index subgroup isomorphic to $\mathbb{Z}$. Let $g \in G \setminus N$. Since N is normal in G, G acts by conjugation on N and hence there exists a group homomorphism $c_g \in \mathrm{Aut}(N) \simeq \{-1, 1\}$. Since $K \subseteq N$ y g acts non-trivially on K,

$$c_g(n) = gng^{-1} = n^{-1}$$

for all $n \in N$. Since $g^2 \in N$,

$$g^2 = gg^2g^{-1} = g^{-2}.$$

Therefore $g^4 = 1$, a contradiction since $g \neq 1$ and G has no torsion. □

Before giving another application of the transfer map, we prove Dietzman's theorem:

theorem:Dietzmann

Theorem 5.4 (Dietzmann). *Let G be a group and $X \subseteq G$ be a finite subset of G closed by conjugation. If there exists n such that $x^n = 1$ for all $x \in X$, then $\langle X \rangle$ is a finite subgroup of G.*

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

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

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

$$s = x(x^{-1}x_1x)(x^{-1}x_2x)\cdots(x^{-1}x_{t-1}x)x_{t+1}\cdots x_m$$

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

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

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

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

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

a contradiction to the minimality of m. □

The second result goes back to Schur:

thm:Schur

Theorem 5.5 (Schur). *Let G be a group. If $Z(G)$ has finite index in G, then $[G,G]$ is finite.*

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

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

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

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

Moreover, X is closed under conjugation, as

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

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

Exercise 5.6. Let G be the group with generators a,b,c and relations $ab = ca$, $ac = ba$ and $bc = ab$. Prove the following statements:

1) G is infinite and non-abelian.
2) $Z(G)$ has finite index in G and every conjugacy class of G is finite.
3) $[G,G]$ is finite.
4) The subgroup $N = \langle a^3 \rangle$ of G generated by a^3 is central and G/N is finite.

We conclude the section with some results similar to that of Schur.

thm:Niroomand

Theorem 5.7 (Niroomand). *If the set of commutators of a group G is finite, then $[G,G]$ is finite.*

Proof. Let $C = \{[x_1,y_1], \dots, [x_k,y_k]\}$ be the (finite) set of commutators of G and $H = \langle x_1, x_2, \dots, x_k, y_1, y_2, \dots, y_k \rangle$. Since C is a set of commutators of H, it follows that $[G,G] = \langle C \rangle \subseteq [H,H]$. To simplify the notation we write $H = \langle h_1, \dots, h_{2k} \rangle$. Since $h \in Z(H)$ if and only if $h \in C_H(h_i)$ for all $i \in \{1, \dots, 2k\}$, we conclude that $Z(H) = C_H(h_1) \cap \cdots \cap C_H(h_{2k})$. Moreover, if $h \in H$, then $hh_ih^{-1} = ch_i$ for some

$c \in C$. Thus the conjugacy class of each h_i contains at most as many elements as C. This implies that

$$|H/Z(H)| = |H/\cap_{i=1}^{2k} C_H(h_i)| \leq \prod_{i=1}^{2k} (H : C_H(h_i)) \leq |C|^{2k}.$$

Since $H/Z(H)$ is finite, $[H,H]$ is finite. Hence $[G,G] = \langle C \rangle \subseteq [H,H]$ is a finite group. □

thm:HiltonNiroomand

Theorem 5.8 (Hilton–Niroomand). *Let G be a finitely generated group. If $[G,G]$ is finite and $G/Z(G)$ is generated by n elements, then*

$$|G/Z(G)| \leq |[G,G]|^n.$$

Proof. Assume that $G/Z(G) = \langle x_1 Z(G), \dots, x_n Z(G) \rangle$. Let

$$f \colon G/Z(G) \to [G,G] \times \cdots \times [G,G], \quad y \mapsto ([x_1,y], \dots, [x_n,y]).$$

Note that f is well-defined: If $y \in G$ y $z \in Z(G)$, then $[x_i,y] = [x_i,yz]$ for all i. Then $f(yz) = f(y)$.

The map f is injective. Assume that $f(xZ(G)) = f(yZ(G))$. Then $[x_i,x] = [x_i,y]$ for all $i \in \{1,\dots,n\}$. For each i we compute

$$\begin{aligned}[x^{-1}y, x_i] &= x^{-1}[y,x_i]x[x^{-1},x_i] \\ &= x^{-1}[y,x_i][x_i,x]x = x^{-1}[x_i,y]^{-1}[x_i,x]x = x^{-1}[x_i,y]^{-1}[x_i,y]x = 1.\end{aligned}$$

This implies that $x^{-1}y \in Z(G)$. Indeed, since every $g \in G$ can be written as $g = x_k z$ for some $k \in \{1,\dots,n\}$ and some $z \in Z(G)$, it follows that

$$[x^{-1}y, g] = [x^{-1}y, x_k z] = [x^{-1}y, x_k] = 1.$$

Since f is injective, $|G/Z(G)| \leq |[G,G]|^n$. □

Exercise 5.9. Prove Theorem 5.8 from Theorem 5.7.

Lecture 5

§6. Bi-ordered groups

Based on Example 2.1 we will study some properties of groups.

Recall that a **total order** is a partial order in which any two elements are comparable. This means that a total order is a binary relation $\leq$ on some set X such that for all $x, y, z \in X$ one has

1) $x \leq x$.
2) $x \leq y$ and $y \leq z$ imply $x \leq z$.
3) $x \leq y$ and $y \leq x$ imply $x = y$.
4) $x \leq y$ or $y \leq x$.

A set equipped with a total order is a **totally ordered set**.

Definition 6.1. A group G is **bi-ordered** if there exists a total order $<$ in G such that $x < y$ implies that $xz < yz$ and $zx < zy$ for all $x, y, z \in G$.

Example 6.2. The group $\mathbb{R}_{>0}$ of positive real numbers is bi-ordered.

The multiplicative group $\mathbb{R} \setminus \{0\}$ is not bi-ordered. Why?

Exercise 6.3. Let G be a bi-ordered group and $x, x_1, y, y_1 \in G$. Prove that $x < y$ and $x_1 < y_1$ imply $xx_1 < yy_1$.

Clearly, bi-orderability is preserved under taking subgroups.

Exercise 6.4. Let G be a bi-ordered group and $g, h \in G$. Prove that $g^n = h^n$ for some $n > 0$ implies $g = h$.

The following result goes back to Neumann.

Exercise 6.5. Let G be a bi-ordered group and $g, h \in G$. Prove that $g^n \in C_G(h)$ if and only if $g \in C_G(h)$.

Bi-ordered groups do not behave nicely under extensions:

xca:BO_sequence

Exercise 6.6. Let $1 \to K \to G \to Q \to 1$ be an exact sequence of groups. Assume that K and Q are bi-ordered. Prove that G is bi-ordered if and only if $x < y$ implies $gxg^{-1} < gyg^{-1}$ for all $x, y \in K$ and $g \in G$.

Definition 6.7. Let G be a bi-ordered group. The **positive cone** of G is the set $P(G) = \{x \in G : 1 < x\}$.

Let us state some properties of positive cones.

pro:biordenableP1

Proposition 6.8. *Let G be a bi-ordered group and let P be its positive cone.*

1) *P is closed under multiplication, i.e. $PP \subseteq P$.*
2) *$G = P \cup P^{-1} \cup \{1\}$ (disjoint union).*
3) *$xPx^{-1} = P$ for all $x \in G$.*

Proof. If $x, y \in P$ and $z \in G$, then, since $1 < x$ and $1 < y$, it follows that $1 < xy$. Thus $1 = z1z^{-1} < zxz^{-1}$. It remains to prove the second claim. If $g \in G$, then $g = 1$ or $g > 1$ or $g < 1$. Note that $g < 1$ if and only if $1 < g^{-1}$, so the claim follows. □

The previous proposition admits a converse statement.

pro:biordenableP2

Proposition 6.9. *Let G be a group and P be a subset of G such that P is closed under multiplication, $G = P \cup P^{-1} \cup \{1\}$ (disjoint union) and $xPx^{-1} = P$ for all $x \in G$. Let $x < y$ whenever $yx^{-1} \in P$. Then G is bi-ordered with positive cone is P.*

Proof. Let $x, y \in G$. Since $yx^{-1} \in G$ and $G = P \cup P^{-1} \cup \{1\}$ (disjoint union), either $yx^{-1} \in P$ or $xy^{-1} = (yx^{-1})^{-1} \in P$ or $yx^{-1} = 1$. Thus either $x < y$ or $y < x$ or $x = y$. If $x < y$ and $z \in G$, then $zx < zy$, as $(zy)(zx)^{-1} = z(yx^{-1})z^{-1} \in P$ and $zPz^{-1} = P$. Moreover, $xz < yz$ since $(yz)(xz)^{-1} = yx^{-1} \in P$. To prove that P is the positive cone of G note that $x1^{-1} = x \in P$ if and only if $1 < x$. □

An important property:

pro:BOsintorsion

Proposition 6.10. *Bi-ordered groups are torsion-free.*

Proof. Let G be a bi-ordered group and $g \in G \setminus \{1\}$. If $g > 1$, then $1 < g < g^2 < \cdots$. If $g < 1$, then $1 > g > g^2 > \cdots$. Hence $g^n \neq 1$ for all $n \neq 0$. □

The converse of the previous proposition does not hold.

Exercise 6.11. Let $G = \langle x, y : yxy^{-1} = x^{-1} \rangle$.

1) Prove that x and y are torsion-free.
2) Prove that G is torsion-free.
3) Prove that $G \simeq \langle a, b : a^2 = b^2 \rangle$.

Example 6.12. The torsion-free group $G = \langle x, y : yxy^{-1} = x^{-1} \rangle$ is not bi-ordered. If not, let P be the positive cone. If $x \in P$, then $yxy^{-1} = x^{-1} \in P$, a contradiction. Hence $x^{-1} \in P$ and $x = y^{-1}x^{-1}y \in P$, a contradiction.

thm:BO **Theorem 6.13.** *Let G be a bi-ordered group. Then $K[G]$ is a domain such that only has trivial units. Moreover, if G is non-trivial, then $J(K[G]) = \{0\}$.*

Proof. Let $\alpha,\beta \in K[G]$ be such that

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

Then

$$g_1h_1 \leq g_ih_j \leq g_mh_n$$

for all i,j. Moreover, $g_1h_1 = g_ih_j$ if and only if $i = j = 1$. The coefficient of g_1h_1 in $\alpha\beta$ is $a_1b_1 \neq 0$. In particular, $\alpha\beta \neq 0$. If $\alpha\beta = \beta\alpha = 1$, then the coefficient of g_mh_n in $\alpha\beta$ is a_mb_n. Hence $m = n = 1$ and therefore $\alpha = a_1g_1$ and $\beta = b_1h_1$ with $a_1b_1 = b_1a_1 = 1$ in K and $g_1h_1 = 1$ in G. □

thm:Levi **Theorem 6.14 (Levi).** *Let A be an abelian group. Then A is bi-ordered if and only if A is torsion-free.*

Proof. If A is bi-ordered, then A is torsion-free. Let us prove the non-trivial implication, so assume that A is torsion-free abelian. Let $\mathcal{S}$ be the class of subsets P of A such that $0 \in P$, are closed under the addition of A and satisfy the following property: if $x \in P$ and $-x \in P$, then $x = 0$. Clearly, $\mathcal{S} \neq \emptyset$, as $\{0\} \in \mathcal{S}$. The inclusion turns $\mathcal{S}$ into a partially ordered set and $\bigcup_{i\in I} P_i$ is an upper bound for the chain $\{P_i : i \in I\}$. By Zorn's lemma, $\mathcal{S}$ admits a maximal element $P \in \mathcal{S}$.

Claim. If $x \in A$ is such that $kx \in P$ for some $k > 0$, then $x \in P$.

Let $Q = \{x \in A : kx \in P \text{ for some } k > 0\}$. We will show that $Q \in \mathcal{S}$. Clearly, $0 \in Q$. Moreover, Q is closed under addition, as $k_1x_1 \in P$ and $k_2x_2 \in P$ imply $k_1k_2(x_1 + x_2) \in P$. Let $x \in A$ be such that $x \in Q$ and $-x \in Q$. Thus $kx \in P$ and $l(-x) \in P$ for some $l > 0$. Since $klx \in P$ and $kl(-x) \in P$, it follows that $klx = 0$, a contradiction since A is torsion-free. Hence $x \in Q \subseteq P$.

Claim. If $x \in A$ is such that $x \notin P$, then $-x \in P$.

Assume that $-x \notin P$ and let $P_1 = \{y + nx : y \in P,\ n \geq 0\}$. We will show that $P_1 \in \mathcal{S}$. Clearly, $0 \in P_1$ and P_1 is closed under addition. If $P_1 \notin S$, there exists

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

where $y_1, y_2 \in P$ and $n_1, n_2 \geq 0$. Thus $y_1 + y_2 = -(n_1 + n_2)x$. If $n_1 = n_2 = 0$, then $y_1 = -y_2 \in P$ and $y_1 = y_2 = 0$, so it follows that $y_1 + n_1x = 0$, a contradiction. If $n_1 + n_2 > 0$, then, since

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

it follows from the first claim that $-x \in P$, a contradiction. Let us show that $P_1 \in \mathcal{S}$. Since $P \subseteq P_1$, the maximality of P implies that $x \in P = P_1$.

By Proposition 6.9, $P^* = P \setminus \{0\}$ is the positive cone of a bi-order in A. In fact, P^* is closed under addition, as $x, y \in P^*$ implies that $x + y \in P$ and $x + y = 0$ implies $x = y = 0$, as $x = -y \in P$. Moreover, $G = P^* \cup -P^* \cup \{0\}$ (disjoint union), as the second claim states that $x \notin P^*$ implies $-x \in P$. □

Our proof of Passman's theorem (Theorem 4.8) used the fact that the group algebra $K[G]$ of a torsion-free abelian group G has no non-zero divisors. We now present a proof of this fact.

cor:domain_G_abelian **Corollary 6.15.** *Let A be a non-trivial torsion-free abelian group. Then $K[A]$ is a domain that only admits trivial units and $J(K[A]) = \{0\}$.*

Proof. Apply Levi's theorem and Theorem 6.13. □

Some exercises. The first one is a variation on Exercise 6.6.

Exercise 6.16. Let N be a central subgroup of G. If N and G/N are bi-ordered, then G is bi-ordered. Prove with an example that N needs to be central, normal is not enough.

Exercise 6.17. Let G be a group that admits a sequence

$$\{1\} = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$$

such that each G_k is normal in G_{k+1} and each quotient G_{k+1}/G_k is torsion-free abelian. Prove that G is bi-ordered.

Exercise 6.18. Prove that torsion-free nilpotent groups are bi-ordered.

§7. Left-ordered groups

Definition 7.1. A group G is **left-ordered** if there is a total order $<$ in G such that $x < y$ implies $xz < yz$ for all $x, y, z \in G$.

If G is left-ordered, the positive cone of G is defined as $P(G) = \{x \in G : 1 < x\}$.

Exercise 7.2. Let G be left-ordered with positive cone P. Prove that P is closed under multiplication and that $G = P \cup P^{-1} \cup \{1\}$ (disjoint union).

xca:LO_cone **Exercise 7.3.** Let G be a group and P be a subset closed under multiplication. Assume that $G = P \cup P^{-1} \cup \{1\}$ (disjoint union). Prove that $x < y$ if and only if $x^{-1}y \in P$ turns G into a left-ordered group with positive cone P.

Left-ordered groups behave nicely with respect to extensions. Let G be a group and N be a left-ordered normal subgroup of G. If $\pi\colon G \to G/N$ is the canonical map and G/N is left-ordered, then G is left-ordered with $x < y$ if and only if either $\pi(x) < \pi(y)$ or $\pi(x) = \pi(y)$ and $1 < x^{-1}y$.

Proposition 7.4. *Let G be a group and N be a normal subgroup of G. If N and G/N are left-ordered, then so is G.*

Proof. Since N and G/N are both left-ordered, there exist positive cones $P(N)$ and $P(G/N)$. Let $\pi\colon G \to G/N$ be the canonical map and

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

A routine calculation shows that $P(G)$ is closed under multiplication and that G decomposes as $G = P(G) \cup P(G)^{-1} \cup \{1\}$ (disjoint union). It follows from Exercise 7.3 that G is left-ordered. □

We now present a criterion for detecting left-ordered groups. We shall need a lemma.

lem:fg

Lemma 7.5. *Let G be a finitely generated group. If H is a finite-index subgroup, then H is finitely generated.*

Proof. Assume that G is generated by $\{g_1, \dots, g_m\}$. Assume that for each i there exists k such that $g_i^{-1} = g_k$. Let $\{t_1, \dots, t_n\}$ be a transversal of H in G. For $i \in \{1, \dots, n\}$ and $j \in \{1, \dots, m\}$ write

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

We claim that H is generated by the $h(i,j)$. For $x \in H$, write

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

where $k_1, \dots, k_{s-1} \in \{1, \dots, n\}$. Since $t_{k_s} \in H$, it follows that $t_{k_s} = t_1 \in H$ and therefore $x \in H$. □

Now the theorem.

Theorem 7.6. *Let G be a finitely generated torsion-free group. If A is an abelian normal subgroup such that G/A is finite and cyclic, then G is left-ordered.*

Proof. Note that if A is trivial, then so is G. Let us assume that $A \neq \{1\}$. Since $(G : A)$ is finite, A is finitely generated by the previous lemma. We proceed by induction on the number of generators of A. Since G/A is cyclic, there exists $x \in G$ such that $G = \langle A, x \rangle$. Then $[x, A] = \langle [x,a] : a \in A \rangle$ is a normal subgroup of G

such that $A/C_A(x) \simeq [x,A]$ (because $a \mapsto [x,a]$ is a group homomorphism $A \to A$ with image $[x,A]$ and kernel $C_A(x)$). If $\pi\colon G \to G/[x,A]$ is the canonical map, then $G/[x,A] = \langle \pi(A), \pi(x)\rangle$ and thus $G/[x,A]$ is abelian, as $[\pi(x),\pi(A)] = \pi[x,A] = 1$. Moreover, $G/[x,A]$ is finitely generated, as G is finitely generated. Since $(G:A) = n$ and G is torsion-free, it follows that $1 \neq x^n \in A$. Hence $x^n \in C_A(x)$ and therefore $1 \leq \operatorname{rank} C_A(x) < \operatorname{rank} A$ (if $\operatorname{rank} C_A(x) = \operatorname{rank} A$, then $[x,A]$ would be a torsion subgroup of A, a contradiction since $x \notin A$). So

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

and hence $\operatorname{rank}(A/[x,A]) \geq 1$. We proved that $A/[x,A]$ is infinite and hence $G/[x,A]$ is infinite.

Since $G/[x,A]$ is infinite, abelian and finitely generated, there exists a normal subgroup H of G such that $[x,A] \subseteq H$ and $G/H \simeq \mathbb{Z}$. The subgroup $B = A \cap H$ is abelian, normal in H and such that H/B is cyclic (because it is isomorphic to a subgroup of G/A). Since $\operatorname{rank} B < \operatorname{rank} A$, the inductive hypothesis implies that H is left-ordered. Hence G is left-ordered. □

Lagrange and Rhemtulla proved that the integral isomorphism problem has an affirmative solution for left-ordered groups. More precisely, if G is left-ordered and H is a group such that $\mathbb{Z}[G] \simeq \mathbb{Z}[H]$, then $G \simeq H$, see [10].

Theorem 7.7 (Malcev–Neumann). *Let G be left-ordered group. Then $K[G]$ has no zero divisors and no non-trivial units.*

Proof. If $\alpha = \sum_{i=1}^{n} a_i g_i \in K[G]$ and $\beta = \sum_{j=1}^{m} b_j h_j \in K[G]$, then

$$\alpha\beta = \sum_{i=1}^{n}\sum_{j=1}^{m} a_i b_j (g_i h_j). \tag{5.1}$$

eq:producto

Without loss of generality we may assume that $a_i \neq 0$ for all i and $b_j \neq 0$ for all j. Moreover, we may assume that $g_1 < g_2 < \cdots < g_n$. Let i, j be such that

$$g_i h_j = \min\{g_i h_j : 1 \leq i \leq n, 1 \leq j \leq m\}.$$

Then $i = 1$, as $i > 1$ implies $g_1 h_j < g_i h_j$, a contradiction. Since $g_1 h_j \neq g_1 h_k$ whenever $k \neq j$, there exists a unique minimal element in the left hand side of Equality (5.1). The same argument shows that there is a unique maximal element in (5.1). Thus $\alpha\beta \neq 0$, as $a_1 b_j \neq 0$, and therefore $K[G]$ has no zero divisors. If, moreover, $n > 1$ or $m > 1$, then (5.1) contains at least two terms than cancel out and thus $\alpha\beta \neq 1$. It follows that units of $K[G]$ are trivial. □

Formanek proved that the zero divisors conjecture is true in the case of torsion-free super solvable. Brown and, independently, Farkas and Snider proved that the conjecture is true in the case of groups algebras (over fields of characteristic zero) of polycyclic-by-finite torsion-free groups. These results can be found in Chapter 13 of Passman's book [12].

§8. The braid group

Definition 8.1. Let $n \geq 1$. The **braid group** $\mathbb{B}_n$ is the group with generators $\sigma_1, \dots, \sigma_{n-1}$ and relations

$$\begin{aligned} &\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} && \text{if } 1 \leq i \leq n-2,\\ &\sigma_i\sigma_j = \sigma_j\sigma_i && \text{if } |i-j| > 1. \end{aligned}$$

Note that $\mathbb{B}_1 = \{1\}$ and $\mathbb{B}_2 \simeq \mathbb{Z}$. The braid group $\mathbb{B}_3$ is generated by σ_1 and σ_2 with relations $\sigma_1\sigma_2\sigma_1 = \sigma_2\sigma_1\sigma_2$.

Exercise 8.2. Prove that there exists a group homomorphism $\mathbb{B}_n \to \mathbb{S}_n$ given by $\sigma_i \mapsto (i\,i+1)$ for all $i \in \{1, \dots, n-1\}$.

Note that if $n \geq 3$, then $\mathbb{B}_n$ is a non-abelian group, as there exists a surjective group homomorphism $\mathbb{B}_n \to \mathbb{S}_n$.

Exercise 8.3. Let $n \geq 2$. Prove that the map $\deg\colon \mathbb{B}_n \to \mathbb{Z}$, $\sigma_i \mapsto 1$, is a group homomorphism. Moreover, $\ker\deg = [\mathbb{B}_n, \mathbb{B}_n]$.

The previous result implies, in particular, that $\mathbb{B}_n$ is an infinite group for all $n \geq 2$. Moreover, $\sigma_i^m \neq 1$ for all $m \in \mathbb{Z} \setminus \{0\}$ and all i.

Exercise 8.4. Prove that $\mathbb{B}_3 \simeq \langle x, y : x^2 = y^3 \rangle$ and that $\mathbb{B}_3/Z(\mathbb{B}_3) \simeq \mathbf{PSL}_2(\mathbb{Z})$.

Exercise 8.5. Prove that the center $Z(\mathbb{B}_3)$ of $\mathbb{B}_3$ is the cyclic group generated by $(\sigma_1\sigma_2\sigma_1)^2$.

More generally, one can prove that the center of $\mathbb{B}_n$ is generated by Δ_n^2, where

$$\Delta_n = (\sigma_1 \cdots \sigma_{n-1})(\sigma_1 \cdots \sigma_{n-2}) \cdots (\sigma_1\sigma_2)\sigma_1,$$

see for example [8, Theorem 1.24]. As a corollary, $\mathbb{B}_n \simeq \mathbb{B}_m$ if and only if $n = m$.

Exercise 8.6. Let $n \geq 3$. Prove that $\mathbb{B}_n$ is not bi-ordered.

One can prove that the natural map $\mathbb{B}_n \to \mathbb{B}_{n+1}$ is an injective group homomorphism, this is not an easy proof (see [8, Corollary 1.14]). Moreover, the diagram

$$\begin{tikzcd} \mathbb{B}_n \arrow[r, two heads] \arrow[d, hook] & \mathbb{S}_n \arrow[d, hook] \\ \mathbb{B}_{n+1} \arrow[r, two heads] & \mathbb{S}_{n+1} \end{tikzcd}$$

commutes.

xca:derivedB3 **Exercise 8.7.** Use the Reidemeister–Schreier's method to prove that $[\mathbb{B}_3, \mathbb{B}_3]$ is isomorphic to the free group in two letters.

A celebrated theorem of Dehornoy states that the braid group $\mathbb{B}_n$ is left-ordered (see for example [8, Theorem 7.15]). The proof of this fact is quite hard. However, there is a nice short proof of the fact that $\mathbb{B}_3$ is left-ordered, see [2, §7.2].

Open problem 8.1 (Burau's representation). Let $\mathbb{B}_4 \to \mathbf{GL}_4(\mathbb{Z}[t,t^{-1}])$ be the group homomorphism given by

$$\sigma_1 \mapsto \begin{pmatrix} 1-t & t & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \sigma_2 \mapsto \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1-t & t & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \sigma_3 \mapsto \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1-t & t \\ 0 & 0 & 1 & 0 \end{pmatrix}.$$

Is this homomorphism injective?

In general, the Burau's representation $\mathbb{B}_n \to \mathbf{GL}_n(\mathbb{Z}[t,t^{-1}])$ is defined by

$$\sigma_j \mapsto I_{j-1} \oplus \begin{pmatrix} 1-t & t \\ 1 & 0 \end{pmatrix} \oplus I_{n-j-1},$$

where I_k denotes the $k \times k$ identity matrix.

It is known that the Burau's representation of $\mathbb{B}_n$ is faithful for $n \leq 3$ and not faithful for $n \geq 5$. Only the case $n = 4$ remains open.

Krammer [9] and Bigelow [1] independently proved that braid groups are linear.

§9. Locally indicable groups

Definition 9.1. A group G is **indicable** if there exists a non-trivial group homomorphism $G \to \mathbb{Z}$.

We know that braid groups are indicable. The free group F_n in n letters is indicable.

Definition 9.2. A group G is **locally indicable** if every non-trivial finitely generated subgroup is indicable.

Burns–Hale's theorem (see [2, Theorem 1.50]) states that a group G is left-ordered if and only if for every non-trivial finitely generated subgroup H of G there exists a left-ordered group L and a non-trivial group homomorphism $H \to L$. As a consequence, locally indicable groups are left-ordered.

Example 9.3. Since subgroups of free groups are free, it follows that F_n is locally indicable.

pro:LI_exact

Proposition 9.4. *Let $1 \to K \to G \to Q \to 1$ be an exact sequence of groups. If K and Q are locally indicable, then G is locally indicable.*

Proof. Let $g_1,\dots,g_n \in G$ and $L = \langle g_1,\dots,g_n\rangle$. Assume that $\beta(L) \neq \{1\}$. Since Q is locally indicable, there exists a non-trivial group homomorphism $\beta(L) \to \mathbb{Z}$. Then the composition $L \to Q \to \mathbb{Z}$ is then a non-trivial group homomorphism. Assume now that $\beta(L) = \{1\}$. Then there exist $k_1,\dots,k_n \in K$ such that $\alpha(k_i) = g_i$ for all $i \in \{1,\dots,n\}$. Note that $\alpha\colon \langle k_1,\dots,k_n\rangle \to L$ is a group isomorphism. Since K is locally indicable, there exits a non-trivial group homomorphism $\langle k_1,\dots,k_n\rangle \to \mathbb{Z}$. Thus the composition $L \to \langle k_1,\dots,k_n\rangle \to \mathbb{Z}$ is a non-trivial group homomorphism and hence G is locally indicable. □

As a consequence of the previous proposition, if G and H are locally indicable groups and $\sigma\colon G \to \mathrm{Aut}(H)$ is a group homomorphism, then $G \rtimes_\sigma H$ is locally indicable. In particular, the direct product of locally indicable groups is locally indicable.

Example 9.5. The group $G = \langle x, y : x^{-1}yx = y^{-1}\rangle$ is locally indicable. We know that G is torsion-free. Let $K = \langle y\rangle \simeq \mathbb{Z}$. Then $G/K \simeq \mathbb{Z}$ and then, since there is an exact sequence $1 \to \mathbb{Z} \to G \to \mathbb{Z} \to 1$ it follows from Proposition 9.4 that G is locally indicable.

xca:B3_LI **Exercise 9.6.** Prove that $\mathbb{B}_3$ is locally indicable.

The previous exercise uses the fact that $[\mathbb{B}_3,\mathbb{B}_3]$ is isomorphic to the free group in two letters, see Exercise 8.7. An alternative solution to the previous fact goes as follows: $\mathbb{B}_3$ is the fundamental group of the trefoil knot and fundamental groups of knots are locally indicable.

Exercise 9.7. Prove that $\mathbb{B}_4$ is locally indicable.

The previous exercise might be harder than Exercise 9.6. One possible solution is based on using the Reidemeister–Schreier method to prove that $[\mathbb{B}_4,\mathbb{B}_4]$ is a certain semidirect product between free groups in two generators. Another solution: Let $f\colon \mathbb{B}_4 \to \mathbb{B}_3$ be the group homomorphism given by $f(\sigma_1) = f(\sigma_3) = \sigma_1$ and $f(\sigma_2) = \sigma_2$. Then $\ker f = \langle \sigma_1\sigma_3^{-1}, \sigma_2\sigma_1\sigma_3^{-1}\sigma_2^{-1}\rangle$ is isomorphic to the free group in two letters. Now use the exact sequence $1 \to \ker f \to \mathbb{B}_4 \to \mathbb{B}_3 \to 1$.

xca:relations **Exercise 9.8.** Let $n \geq 5$. Consider the elements of $\mathbb{B}_n$ given by

$$\beta_1 = \sigma_1^{-1}\sigma_2, \quad \beta_2 = \sigma_2\sigma_1^{-1}, \quad \beta_3 = \sigma_1\sigma_2\sigma_1^{-2}, \quad \beta_4 = \sigma_3\sigma_1^{-1}, \quad \beta_5 = \sigma_4\sigma_1^{-1}.$$

Prove the following relations:

1) $\beta_1\beta_5 = \beta_5\beta_2$.
2) $\beta_2\beta_5 = \beta_5\beta_3$.
3) $\beta_1\beta_3 = \beta_2$.
4) $\beta_1\beta_4\beta_3 = \beta_4\beta_2\beta_4$.
5) $\beta_4\beta_5\beta_4 = \beta_5\beta_4\beta_5$.

Exercise 9.9. Let $n \geq 5$. Prove that $\mathbb{B}_n$ is not locally indicable.

For the previous exercise one needs to show that every group homomorphism $f\colon \langle \beta_1,\dots,\beta_5\rangle \to \mathbb{Z}$ is trivial. Hint: consider the abelianization of $\langle \beta_1,\dots,\beta_5\rangle$.

§10. Unique product groups

Let G be a group and $A, B \subseteq G$ be non-empty subsets. An element $g \in G$ is a **unique product** in AB if $g = ab = a_1 b_1$ for some $a, a_1 \in A$ and $b, b_1 \in B$ implies that $a = a_1$ and $b = b_1$.

Definition 10.1. A group G has the **unique product property** if for every finite non-empty subsets $A, B \subseteq G$ there exists at least one unique product in AB.

Proposition 10.2. *Left-ordered groups have the unique product property.*

Proof. Let G be a left-ordered group. Let $A = \{a_1, \dots, a_n\} \subseteq G$ and $B \subseteq G$ non-empty and finite. Assume that $a_1 < a_2 < \cdots < a_n$. Let $c \in B$ be such that $a_1 c$ is the minimum of $a_1 B = \{a_1 b : b \in B\}$. We claim that $a_1 c$ admits a unique representation of the form $\alpha\beta$ with $\alpha \in A$ and $\beta \in B$. If $a_1 c = ab$, then, since $ab = a_1 c \leq a_1 b$, it follows that $a \leq a_1$. Hence $a = a_1$ and $b = c$. □

Exercise 10.3. Prove that groups with the unique product property are torsion-free.

The converse does not hold. Promislow's group is a celebrated counterexample.

Theorem 10.4 (Promislow). *The group* $G = \langle a, b : a^{-1}b^2a = b^{-2}, b^{-1}a^2b = a^{-2}\rangle$ *does not have the unique product property.*

Proof. Let

$$S = \{a^2b, b^2a, aba^{-1}, (b^2a)^{-1}, (ab)^{-2}, b, (ab)^2x, (ab)^2, (aba)^{-1}, bab, b^{-1}, a, aba, a^{-1}\}. \tag{5.2}$$

eq:Promislow

We use GAP and the representation $G \to \mathbf{GL}(4, \mathbb{Q})$ given by

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

to check that G does not have unique product property, as each

$$s \in S^2 = \{s_1 s_2 : s_1, s_2 \in S\}$$

admits at least two different decompositions of the form $s = xy = uv$ for $x, y, u, v \in S$. We first create the matrix representations of a and b.

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

Now we create a function that produces the set S.

```
gap> Promislow := function(x, y)
> return Set([
> x^2*y,
> y^2*x,
> x*y*Inverse(x),
> (y^2*x)^(-1),
> (x*y)^(-2),
> y,
> (x*y)^2*x,
> (x*y)^2,
> (x*y*x)^(-1),
> y*x*y,
> y^(-1),
> x,
> x*y*x,
> x^(-1)
]);
end;;
```

So the set S of (5.2) will be `Promislow(a,b)`. We now create a function that checks whether every element of a Promislow subset admits more than one representation.

```
gap> is_UPP := function(S)
> local l,x,y;
> l := [];
> for x in S do
> for y in S do
> Add(l,x*y);
> od;
> od;
> if ForAll(Collected(l), x->x[2] <> 1) then
> return false;
> else
> return fail;
> fi;
> end;;
```

Finally, we check whether every element of S admits more than one representation.

```
gap> S := Promislow(a,b);;
gap> is_UPP(S);
false
```

This completes the proof. $\square$

There are other examples.

Definition 10.5. A group G has the **double property of unique products** if for every finite non-empty subsets $A, B \subseteq G$ such that $|A| + |B| > 2$ there are at least two unique products in AB.

theorem:Strojnowski

Theorem 10.6 (Strojnowski). *Let G be a group. The following statements are equivalent:*

1) *G has the double property of unique products.*
2) *For every non-empty finite subset $A \subseteq G$ contains at least one unique product in $AA = \{a_1a_2 : a_1, a_2 \in A\}$.*
3) *G has the unique product property.*

Proof. It is trivial that 1) $\implies$ 2) es trivial. Let us prove that 2) $\implies$ 3). If G does not have the unique product property, there exist finite non-empty subsets $A, B \subseteq G$ such that every element of AB admits at least two representations. Let $C = AB$. Every element $c \in C$ is of the form $c = (a_1b_1)(a_2b_2)$ for some $a_1, a_2 \in A$ and $b_1, b_2 \in B$. Since $a_2^{-1}b_1^{-1} \in AB$, there exist $a_3 \in A \setminus \{a_2\}$ and $b_3 \in B \setminus \{b_1\}$ such that $a_2^{-1}b_1^{-1} = a_3^{-1}b_3^{-1}$. Thus $b_1a_2 = b_3a_3$ and hence

$$c = (a_1b_1)(a_2b_2) = (a_1b_3)(a_3b_2)$$

has two different representations in AB, as $a_2 \neq a_3$ and $b_1 \neq b_3$.

We now prove that 3) $\implies$ 1). Let us assume that G has the unique product property but it is not a group with double unique products. Then there exist finite non-empty subsets $A, B \subseteq G$ with $|A| + |B| > 2$ such that in AB there exists a unique element ab with a unique representation in AB. Let $C = a^{-1}A$ and $D = Bb^{-1}$. Then $1 \in C \cap D$ and the identity 1 admits a unique representation in CD (because $1 = cd$ with $c = a^{-1}a_1 \neq 1$ and $d = b_1b^{-1} \neq 1$ imply that $ab = a_1b_1$ with $a \neq a_1$ and $b \neq b_1$). Let $E = D^{-1}C$ and $F = DC^{-1}$. Every element of the set EF can be written as $(d_1^{-1}c_1)(d_2c_2^{-1})$. If either $c_1 \neq 1$ or $d_2 \neq 1$, then $c_1d_2 = c_3d_3$ for some elements $c_3 \in C \setminus \{c_1\}$ and $d_3 \in D \setminus \{d_2\}$. Thus $(d_1^{-1}c_1)(d_2c_2^{-1}) = (d_1^{-1}c_3)(d_3c_2^{-1})$ are two different representations for $(d_1^{-1}c_1)(d_2c_2^{-1})$. If either $c_2 \neq 1$ or $d_1 \neq 1$, then $c_2d_1 = c_4d_4$ for some $d_4 \in D \setminus \{d_1\}$ and some $c_4 \in C \setminus \{c_2\}$. Since $d_1^{-1}c_2^{-1} = d_4^{-1}c_4^{-1}$, it follows that

$$(d_1^{-1}1)(1c_2^{-1}) = (d_4^{-1}1)(1c_4^{-1}).$$

Since $|C| + |D| > 2$, either C or D contains $c \neq 1$. Thus $(1 \cdot 1)(1 \cdot 1) = (1 \cdot c)(1 \cdot c^{-1})$. Therefore every element of EF admits at least two representations. □

Exercise 10.7. Prove that if a group G satisfies the unique product property, then $K[G]$ contains only trivial units.

In general it is extremely hard to check whether a given group has the unique product property. As a geometrical way to attack this problem, Bowditch introduced *diffuse groups*. If G is a torsion-free group and $A \subseteq G$ is a subset, we say that A is antisymmetric if $A \cap A^{-1} \subseteq \{1\}$, where $A^{-1} = \{a^{-1} : a \in A\}$. The set of **extremal elements** of A is defined as $\Delta(A) = \{a \in A : Aa^{-1} \text{ is antisymmetric}\}$. Thus

$$a \in A \setminus \Delta(A) \iff \text{there existes } g \in G \setminus \{1\} \text{ such that } ga \in A \text{ and } g^{-1}a \in A.$$

Definition 10.8. A group G is **diffuse** if for every subset $A \subseteq G$ such that $2 \leq |A| < \infty$ one has $|\Delta(A)| \geq 2$.

Proposition 10.9. *Left-ordered groups are diffuse.*

Proof. Let G be a left-ordered group and $A = \{a_1, \dots, a_n\}$ be such that

$$a_1 < a_2 < \cdots < a_n.$$

We claim that $\{a_1, a_n\} \subseteq \Delta(A)$. If $a_1 \in A \setminus \Delta(A)$, there exists $g \in G \setminus \{1\}$ such that $ga_1 \in A$ and $g^{-1}a_1 \in A$. Thus $a_1 \leq ga_1$ and $a_1 \leq g^{-1}a_1$. It follows that $1 \leq a^{-1}ga_1$ and $1 \leq a_1^{-1}g^{-1}a_1 = (a_1^{-1}ga_1)^{-1}$, a contradiction. Similarly, $a_n \in \Delta(A)$. □

pro:difuso=>2up **Proposition 10.10.** *Diffuse groups have the double unique products.*

Proof. Let G be a diffuse group that does not have double unique products. There exist non-empty subsets $A, B \subseteq G$ with $|A|+|B| > 2$ such that $C = AB$ admits at most one unique product. Then $|C| \geq 2$. Since G is diffse, $|\Delta(C)| \geq 2$. If $c \in \Delta(C)$, then c admits a unique expression of the form $c = ab$ with $a \in A$ and $b \in B$ (otherwise, if $c = a_0b_0 = a_1b_1$ with $a_0 \neq a_1$ and $b_0 \neq b_1$). If $g = a_0a_1^{-1}$, then $g \neq 1$,

$$gc = a_0a_1^{-1}a_1b_1 = a_0b_1 \in C.$$

Moreover, $g^{-1}c = a_1a_0^{-1}a_0b_0 = a_1b_0 \in C$. Hence $c \notin \Delta(c)$, a contradiction. □

Open problem 10.1. Find a non-diffuse group with the unique product property.

§11. Connel's theorem

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

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

lemma:sumN **Lemma 11.1.** *Let N be a finite normal subgroup of G. Then $\widehat{N} = \sum_{x \in N} x$ is central in $K[G]$ and $\widehat{N}(\widehat{N} - |N|1) = 0$.*

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

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

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

Si G es un grupo, consideramos el subconjunto

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

lem:DcharG **Lemma 11.2.** *Si G es un grupo, entonces $\Delta^+(G)$ es un subgrupo característico de G.*

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

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

lem:Connel

Lemma 11.3. *Sea G un grupo y sea $x \in \Delta^+(G)$. Existe entonces un subgrupo finito H normal en G tal que $x \in H$.*

Dejamos la demostración como ejercicio ya que el muy similar a lo que hicimos en la demostración del lema 11.2.

thm:Connel

Theorem 11.4 (Connell). *Supongamos que el cuerpo K es de característica cero. Sea G un grupo. Las siguientes afirmaciones son equivalentes:*

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

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

Demostremos ahora que (2) $\implies$ (3). Sea N un subgrupo normal finito. Por el lema 11.1, $\widehat{N} = \sum_{x \in N} x$ es central en $K[G]$ y $\widehat{N}(\widehat{N} - |N|1) = 0$. Como $\widehat{N} \neq 0$ (pues K tiene característica cero) y $Z(K[G])$ es un dominio, $\widehat{N} = |N|1$, es decir: $N = \{1\}$.

Demostremos que (3) $\implies$ (4). Sea $x \in \Delta^+(G)$. Por el lema 11.3 sabemos que existe un subgrupo finito H normal en G que contiene a x. Como por hipótesis H es trivial, se concluye que $x = 1$.

Finalmente demostramos que (4) $\implies$ (1). Sean A y B ideales de $K[G]$ tales que $AB = 0$. Supongamos que $B \neq 0$ y sea $\beta \in B \setminus \{0\}$. Si $\alpha \in A$, entonces, como $\alpha K[G]\beta \subseteq \alpha B \subseteq AB = 0$, el lema 4.7 de Passman implica que $\pi_{\Delta(G)}(\alpha)\pi_{\Delta(G)}(\beta) = 0$. Como por hipótesis $\Delta^+(G)$ es trivial, sabemos que $\Delta(G)$ es libre de torsión y luego $\Delta(G)$ es abeliano por el lema **??**. Esto nos dice que $K[\Delta(G)]$ no tiene divisores de cero y luego $\alpha = 0$. Demostramos entonces que $B \neq 0$ implica que $A = 0$. □

Theorem 11.5 (Connel). *Sea K un cuerpo de característica cero y sea G un grupo. Entonces $K[G]$ es artiniano a izquierda si y sólo si G es finito.*

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

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

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

Lecture 6

§12. The Yang–Baxter equation

We now briefly discuss set-theoretic solutions to the Yang–Baxter equation.

Definition 12.1. A *set-theoretic solution* to the Yang–Baxter equation (YBE) is a pair (X,r), where X is a non-empty set and $r\colon X\times X\to X\times X$ is a bijective map that satisfies

$$(r\times\mathrm{id})(\mathrm{id}\times r)(r\times\mathrm{id})=(\mathrm{id}\times r)(r\times\mathrm{id})(\mathrm{id}\times r),$$

where, if $r(x,y)=(\sigma_x(y),\tau_y(x))$, then

$$\begin{aligned} r\times\mathrm{id}\colon X\times X\times X\to X\times X\times X, &\qquad (r\times\mathrm{id})(x,y,z)=(\sigma_x(y),\tau_y(x),z),\\ \mathrm{id}\times r\colon X\times X\times X\to X\times X\times X, &\qquad (\mathrm{id}\times r)(x,y,z)=(x,\sigma_y(z),\tau_z(y)). \end{aligned}$$

The solution (X,r) is said to be *finite* if X is a finite set.

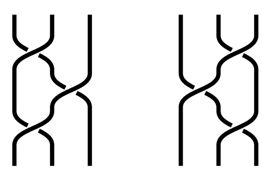

fig:braid

Figure 6.1: The Yang–Baxter equation.

Example 12.2. Let X be a non-empty set. Then (X,id) is a set-theoretic solution to the YBE.

Example 12.3. Let X be a non-empty set. Then (X,r), where $r(x,y)=(y,x)$, is a set-theoretic solution to the YBE. This solution is known as the *trivial solution* over the set X.

By convention, we write

$$r(x,y) = (\sigma_x(y), \tau_y(x)).$$

lem:YB **Lemma 12.4.** *Let X be a non-empty set and $r\colon X\times X \to X\times X$ be a bijective map. Then (X,r) is a set-theoretic solution to the YBE if and only if*

$$\sigma_x\sigma_y = \sigma_{\sigma_x(y)}\sigma_{\tau_y(x)}, \quad \sigma_{\tau_{\sigma_y(z)}(x)}\tau_z(y) = \tau_{\sigma_{\tau_y(x)}(z)}\sigma_x(y), \quad \tau_z\tau_y = \tau_{\tau_z(y)}\tau_{\sigma_y(z)}$$

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

Proof. We write $r_1 = r\times \mathrm{id}$ and $r_2 = \mathrm{id}\times r$. We first compute

$$\begin{aligned} r_1r_2r_1(x,y,z) &= r_1r_2(\sigma_x(y),\tau_y(x),z) = r_1(\sigma_x(y),\sigma_{\tau_y(x)}(z),\tau_z\tau_y(x)) \\ &= \left(\sigma_{\sigma_x(y)}\sigma_{\tau_y(x)}(z), \tau_{\sigma_{\tau_y(x)}(z)}\sigma_x(y), \tau_z\tau_y(x)\right). \end{aligned}$$

Then we compute

$$\begin{aligned} r_2r_1r_2(x,y,z) &= r_2r_1(x,\sigma_y(z),\tau_z(y)) = r_2(\sigma_x\sigma_y(z),\tau_{\sigma_y(z)}(x),\tau_z(y)) \\ &= \left(\sigma_x\sigma_y(z), \sigma_{\tau_{\sigma_y(z)}(x)}\tau_z(y), \tau_{\tau_z(y)}\tau_{\sigma_y(z)}(x)\right) \end{aligned}$$

and the claim follows. □

If (X,r) is a set-theoretic solution, by definition the map $r\colon X\times X\to X\times X$ is invertible. By convention, we write

$$r^{-1}(x,y) = (\widehat{\sigma}_x(y), \widehat{\tau}_y(x)).$$

Note that this implies that

$$x = \widehat{\sigma}_{\sigma_x(y)}\tau_y(x), \quad y = \widehat{\tau}_{\tau_y(x)}\sigma_x(y).$$

It is easy to check that (X,r^{-1}) is a set-theoretic solution to the YBE. Thus Lemma 12.4 implies that the following formulas hold:

$$\widehat{\tau}_y\widehat{\tau}_x = \widehat{\tau}_{\tau_y(x)}\widehat{\tau}_{\sigma_x(y)}, \quad \widehat{\sigma}_x\widehat{\sigma_y} = \widehat{\sigma}_{\sigma_x(y)}\widehat{\sigma}_{\tau_y(x)}.$$

Example 12.5. Let $X = \{1,2,3,4\}$ and $r(x,y) = (\sigma_x(y),\tau_y(x))$, where

$$\begin{aligned} &\sigma_1 = (132), && \sigma_2 = (124), && \sigma_3 = (143), && \sigma_4 = (234), \\ &\tau_1 = (12)(34), && \tau_2 = (12)(34), && \tau_3 = (12)(34), && \tau_4 = (12)(34). \end{aligned}$$

Then r is invertible with $r^{-1}(x,y) = (\widehat{\sigma}_x(y),\widehat{\tau}_y(x))$ given by

$$\begin{aligned} &\widehat{\sigma}_1 = (12)(34), && \widehat{\sigma}_2 = (12)(34), && \widehat{\sigma}_3 = (12)(34), && \widehat{\sigma}_4 = (12)(34), \\ &\widehat{\tau}_1 = (142), && \widehat{\tau}_2 = (123), && \widehat{\tau}_3 = (243), && \widehat{\tau}_4 = (134). \end{aligned}$$

Definition 12.6. A *homomorphism* between the set-theoretic solutions (X,r) and (Y,s) is a map $f\colon X\to Y$ such that the diagram

$$\begin{tikzcd} X\times X \arrow[r, "r"] \arrow[d, "f\times f"'] & X\times X \arrow[d, "f\times f"] \\ Y\times Y \arrow[r, "s"'] & Y\times Y \end{tikzcd}$$

is commutative, that is $s(f\times f)=(f\times f)r$. An *isomorphism* of solutions is a bijective homomorphism of solutions.

Since we are interested in studying the combinatorics behind set-theoretic solutions to the YBE, it makes sense to study the following family of solutions.

Definition 12.7. We say that a set-theoretic solution (X,r) to the YBE is *non-degenerate* if the maps σ_x and τ_x are permutations of X.

By convention, a *solution* we will mean a non-degenerate **set-theoretic** solution to the YBE.

lem:LYZ **Lemma 12.8.** *Let (X,r) be a solution.*

1) *Given $x,u\in X$, there exist unique $y,v\in X$ such that $r(x,y)=(u,v)$.*
2) *Given $y,v\in X$, there exist unique $x,u\in X$ such that $r(x,y)=(u,v)$.*

Proof. For the first claim take $y=\sigma_x^{-1}(u)$ and $v=\tau_y(x)$. For the second, $x=\tau_y^{-1}(v)$ and $u=\sigma_x(y)$. □

The bijectivity of r means that any row determines the whole square. Lemma 12.8 means that any column also determines the whole square, see Figure 6.2.

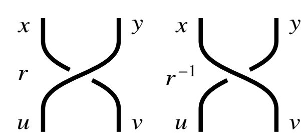

fig:braid **Figure 6.2:** Any row or column determines the whole square.

Example 12.9. If the map $(x,y)\mapsto(\sigma_x(y),\tau_y(x))$ satisfies the Yang–Baxter equation, then so does $(x,y)\mapsto(\tau_x(y),\sigma_y(x))$.

exa:Lyubashenko **Example 12.10.** Let X be a non-empty set and σ and τ be bijections on X such that $\sigma\circ\tau=\tau\circ\sigma$. Then (X,r), where $r(x,y)=(\sigma(y),\tau(x))$, is a non-degenerate solution. This is known as the *permutation solution* associated with permutations σ and τ.

exa:Venkov **Example 12.11.** Let G be a group. Then (G,r), where $r(x,y)=(xyx^{-1},x)$, is a solution.

Example 12.12. Let $n \geq 2$ and $X = \mathbb{Z}/(n)$ be the ring of integers modulo n. Prove that the map $r(x,y) = (2x - y, x)$ satisfies the the set-theoretic YBE.

The following result was proved by Lu, Yan and Zhu.

thm:LYZ **Theorem 12.13 (Lu–Yan–Zhu).** *Let G be a group, $\xi\colon G\times G \to G$, $\xi(x,y) = x \triangleright y$, be a left action of the group G on itself as a set and $\eta\colon G\times G\to G$, $\eta(x,y) = x \triangleleft y$, be a right action of the group G on itself as a set. If the compatibility condition*

$$uv = (u \triangleright v)(u \triangleleft v)$$

holds for all $u, v \in G$, then the pair (G, r), where

$$r\colon G\times G \to G\times G, \quad r(u,v) = (u \triangleright v, u \triangleleft v)$$

is a solution. Moreover, if $r(x,y) = (u,v)$, then

$$r(x^{-1}, y^{-1}) = (u^{-1}, v^{-1}), \quad r(x^{-1}, u) = (y, v^{-1}), \quad r(v, y^{-1}) = (u^{-1}, x).$$

Proof. We write $r_1 = r \times \mathrm{id}$ and $r_2 = \mathrm{id}\times r$. Let

$$r_1r_2r_1(u,v,w) = (u_1, v_1, w_1), \quad r_2r_1r_2(u,v,w) = (u_2, v_2, w_2).$$

The compatibility condition implies that $u_1v_1w_1 = u_2v_2w_2$. So we need to prove that $u_1 = u_2$ and $w_1 = w_2$. We note that

$$\begin{aligned} u_1 &= (u \triangleright v) \triangleright ((u \triangleleft v) \triangleright w), & w_1 &= (u \triangleleft v) \triangleleft w, \\ u_2 &= u \triangleright (v \triangleright w), & w_2 &= (u \triangleleft (v \triangleright w)) \triangleleft (v \triangleleft w). \end{aligned}$$

Using the compatibility condition and the fact that ξ is a left action,

$$u_1 = ((u \triangleright v)(u \triangleleft v)) \triangleright w = (uv) \triangleright w = u \triangleright (v \triangleright w) = u_2.$$

Similarly, since η is a right action,

$$w_2 = u \triangleleft ((v \triangleright w)(v \triangleleft w)) = u \triangleleft (vw) = (u \triangleleft v) \triangleleft w = w_1.$$

To prove that r is invertible we proceed as follows. Write $r(u,v) = (x,y)$, thus $u \triangleright v = x$, $u \triangleleft v = y$ and $uv = xy$. Since

$$(y \triangleright v^{-1})u = (y \triangleright v^{-1})(y \triangleleft v^{-1}) = yv^{-1} = x^{-1}u,$$

it follows that $y \triangleright v^{-1} = x^{-1}$, i.e. $v^{-1} = y^{-1} \triangleright x^{-1}$. Similarly,

$$v(u^{-1} \triangleleft x) = (u^{-1} \triangleright x)(u^{-1} \triangleleft x) = u^{-1}x = vy^{-1}$$

implies that $u^{-1} = y^{-1} \triangleleft x^{-1}$. Clearly $r^{-1} = \zeta(i\times i)r(i\times i)\zeta$, is the inverse of r, where $\zeta(x,y) = (y,x)$ and $i(x) = x^{-1}$. $\square$

Proposition 12.14. *Under the assumptions of Theorem 12.13, if $r(x,y)=(u,v)$, then*

$$r(v^{-1},u^{-1})=(y^{-1},x^{-1}),\quad r(x^{-1},u)=(y,v^{-1}),\quad r(v,y^{-1})=(u^{-1},x).$$

Proof. In the proof of Theorem 12.13 we found that the inverse of the map r is given by $r^{-1}=\zeta(i\times i)r(i\times i)\zeta$, where $\zeta(x,y)=(y,x)$ and $i(x)=x^{-1}$. Hence

$$r^{-1}(y^{-1},x^{-1})=\zeta(i\times i)r(i\times i)\zeta(y^{-1},x^{-1})=\zeta(i\times i)r(x,y)=(v^{-1},u^{-1}).$$

It follows that $r(v^{-1},u^{-1})=(y^{-1},x^{-1})$. To prove the equality $r(x^{-1},u)=(y,v^{-1})$ we proceed as follows. Since $r(x,y)=(u,v)$, it follows that $x\triangleright y=u$. Then $x^{-1}\triangleright u=y$ and hence $r(x^{-1},u)=(y,z)$ for some $z\in G$. Since $xy=uv$ and $x^{-1}u=yz$, it immediately follows that $yt=yv^{-1}$. Then $z=v^{-1}$. Similarly one proves $r(v,y^{-1})=(u^{-1},x)$. $\square$

References

1. S. J. Bigelow. Braid groups are linear. *J. Amer. Math. Soc.*, 14(2):471–486, 2001.
2. A. Clay and D. Rolfsen. *Ordered groups and topology*, volume 176 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2016.
3. The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.11.1*, 2021.
4. D. García-Lucas, L. Margolis, and A. del Río. Non-isomorphic 2-groups with isomorphic modular group algebras. *J. Reine Angew. Math.*, 783:269–274, 2022.
5. G. Gardam. A counterexample to the unit conjecture for group rings. *Ann. of Math. (2)*, 194(3):967–979, 2021.
6. B. J. Gardner and R. Wiegandt. *Radical theory of rings*, volume 261 of *Monographs and Textbooks in Pure and Applied Mathematics*. Marcel Dekker, Inc., New York, 2004.
7. M. Hertweck. A counterexample to the isomorphism problem for integral group rings. *Ann. of Math. (2)*, 154(1):115–138, 2001.
8. C. Kassel and V. Turaev. *Braid groups*, volume 247 of *Graduate Texts in Mathematics*. Springer, New York, 2008. With the graphical assistance of Olivier Dodane.
9. D. Krammer. Braid groups are linear. *Ann. of Math. (2)*, 155(1):131–156, 2002.
10. R. H. Lagrange and A. H. Rhemtulla. A remark on the group rings of order preserving permutation groups. *Canad. Math. Bull.*, 11:679–680, 1968.
11. T. Y. Lam. *A first course in noncommutative rings*, volume 131 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991.
12. D. S. Passman. *The algebraic structure of group rings*. Robert E. Krieger Publishing Co., Inc., Melbourne, FL, 1985. Reprint of the 1977 original.
13. J.-P. Serre. *Finite groups: an introduction*, volume 10 of *Surveys of Modern Mathematics*. International Press, Somerville, MA; Higher Education Press, Beijing, 2016. With assistance in translation provided by Garving K. Luli and Pin Yu.

Index