Leandro Vendramin

Non-commutative algebra

Notes

Sunday 12th February, 2023

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 [13] and Passman's book [14].

Thanks go to Arjen Elbert Dujardin and Robynn Corveleyn.

This version was compiled on Sunday 12th February, 2023 at 15:41.

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 [8].

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 [5]. 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 $g\in G$.

xca:non_trivial:C2 **Exercise 2.2.** Prove that $\mathbb{C}[C_2]$ has non-trivial units.

xca:non_trivial:C5 **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 [6] in the case of K the field of two elements. We will present Gardam's theorem as a computer calculation. We will use GAP [4].

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 [6].

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 $(a_1, \dots, a_n)(b_1, \dots, b_n) = (a_1b_1, \dots, a_nb_n)$ 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 [7, 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. Let K be a field of characteristic two. Prove that $K[C_4]$ contains non-trivial zero divisors and every idempotent of $K[C_4]$ is trivial. What happens if the characteristic of K is not two?

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 $1 - \alpha h = 1 - h + \lambda g h$ 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 $n_1 + \dots + n_k = n$ 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

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

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

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

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

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*

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

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

$$H_1b\cap\left(\bigcup_{j=1}^{n}H_1a_{1j}\right)=\emptyset.$$

Since $H_1b\subseteq\bigcup_{i=2}^{m}\bigcup_{j=1}^{n}H_ia_{ij}$, it follows that

$$H_1a_{1k}\subseteq\bigcup_{i=2}^{m}\bigcup_{j=1}^{n}H_1a_{ij}b^{-1}a_{1k}.$$

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

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

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 [15, 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

$$s = x_1x_2\cdots x_{t-1}xx_{t+1}\cdots x_m,$$

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

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

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 $zx < zy$ 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

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

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 $t_{k_s} = t_1 \in H$. □

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 [12].

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 $\alpha=\sum_{i=1}^n a_ig_i\in K[G]$ and $\beta=\sum_{j=1}^m b_jh_j\in K[G]$, then

$$\alpha\beta=\sum_{i=1}^n\sum_{j=1}^m a_ib_j(g_ih_j). \tag{5.1}$$ 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

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

Then $i=1$, as $i>1$ implies $g_1h_j<g_ih_j$, a contradiction. Since $g_1h_j\neq g_1h_k$ 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 $a_1b_j\neq 0$, 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 [14].

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

xca:Bn_notBO **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 [9, 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 [9, 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 [3, §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.

Using a different representation, Krammer [11] and Bigelow [2] independently proved that braid groups are linear.

Lecture 6

§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 [3, 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.

There are groups that are left-ordered and not locally indicable, see for example [1]. The braid group $\mathbb{B}_n$ for $n \geq 5$ is another example of a left-ordered group that is not locally indicable.

pro:LI_exact

Proposition 9.4. *Let*

$$1 \longrightarrow K \xrightarrow{\alpha} G \xrightarrow{\beta} Q \longrightarrow 0$$

be an exact sequence of groups and group homomorphisms. 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 first 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 $L \to \beta(Q) \to \mathbb{Z}$ 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. $\square$

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 $G \ltimes_\sigma H$ 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 be a non-empty finite subset of G and $B = \{b_1, \dots, b_n\} \subseteq G$. Assume that $b_1 < b_2 < \cdots < b_n$. Let $c \in A$ be such that cb_1 is the minimum of $Ab_1 = \{ab_1 : a \in A\}$. We claim that cb_1 admits a unique representation of the form $\alpha\beta$ with $\alpha \in A$ and $\beta \in B$. If $cb_1 = ab$, then, since $ab = cb_1 \leq ab_1$, it follows that $b \leq b_1$. Hence $b = b_1$ and $a = c$. □

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

$$S = \{a^2b, b^2a, aba^{-1}, (b^2a)^{-1}, (ab)^{-2}, b, (ab)^2a, (ab)^2, (aba)^{-1}, \\ bab, b^{-1}, a, aba, a^{-1}\}. \quad (6.1)$$

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 (6.1) 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^2 admits more than one representation.

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

This completes the proof. □

xca:A1Bm **Exercise 10.5.** Let G be a group and $A, B \subseteq G$ be finite non-empty subsets. Prove that if $|A| = 1$, then AB contains a unique product.

The size of the set A can be extended.

xca:gABh **Exercise 10.6.** Let G be a group and $A, B \subseteq G$ be finite non-empty subsets. Prove that AB has no unique products if and only if $(gA)(Bh)$ has no unique product for all $g, h \in G$.

xca:A2Bm

Exercise 10.7. Let G be a torsion-free group and $A,B \subseteq G$ be finite non-empty subsets. Prove that if $|A|=2$, then AB contains a unique product.

The case where the set A has size three is still open. One can prove, for example, that if $|A|=3$, then $|B| \geq 7$.

Definition 10.8. 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 10.9 (Strojnowski). *Let G be a group. The following statements are equivalent:*

1) *G has the double property of unique products.*
2) *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).

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 10.10. 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 $\Delta(A) = \{a \in A : Aa^{-1}$ 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 10.11. A group G is **diffuse** if for every finite subset $A \subseteq G$ such that $2 \leq |A| < \infty$ one has $|\Delta(A)| \geq 2$.

This means that a group G is diffuse if for every finite non-empty subset $A \subseteq G$ there exists $a \in A$ such that for all $g \in G \setminus \{1\}$ either $ga \notin A$ or $g^{-1}a \notin A$.

Proposition 10.12. *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, $a_n \in \Delta(A)$. □

There are diffuse groups that are not left-ordered, see [10].

pro:difuso=>2up

Proposition 10.13. *Diffuse groups have 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.

Lecture 7

§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 $\widehat{N}\widehat{N}=\sum_{j=1}^k n_j\widehat{N}=|N|\widehat{N}$. $\square$

If G is a group, let

$$\Delta^+(G)=\{x\in\Delta(G):x\text{ has finite order}\}.$$

An application of Dietzmann's theorem:

lem:DcharG

Proposition 11.2. *If G is a group, then $\Delta^+(G)$ is a characteristic subgroup of G.*

Proof. Clearly, $1\in\Delta^+(G)$. Let $x,y\in\Delta^+(G)$ and H be the subgroup of G generated by the set C formed by all finite conjugates of x and y. If $|x|=n$ and $|y|=m$, then $c^{nm}=1$ for all $c\in C$. Since C is finite and closed under conjugation, Dietzmann's theorem implies that H is finite and hence $H\subseteq\Delta^+(G)$. In particular, $xy^{-1}\in\Delta^+(G)$. It is now clear that $\Delta^+(G)$ is a characteristic subgroup, as for every $f\in\operatorname{Aut}(G)$ and $x\in\Delta^+(G)$ it follows that $f(x)\in\Delta^+(G)$. $\square$

To prove Connel's theorem we need a lemma.

lem:Connel **Lemma 11.3.** *Let G be a group and $x \in \Delta^+(G)$. There exists a finite normal subgroup H of G such that $x \in H$.*

Proof. Let H be the subgroup generated by the conjugates of x. Since x has finitely many conjugates, H is finitely generated. Moreover, H is normal in G and it is generated by torsion elements. All these generators of H have the same order, say n. By Dietzmann's theorem, H is finite. □

Recall that a ring R is said to be **prime** if for $x, y \in R$ such that $xRy = \{0\}$ it follows that $x = 0$ or $y = 0$. Prime rings are non-commutative analogs of domains.

thm:Connel **Theorem 11.4 (Connell).** *Let K be a field of characteristic zero. Let G be a group. The following statements are equivalent:*

1) *$K[G]$ is prime.*
2) *$Z(K[G])$ is prime.*
3) *G does not contain non-trivial finite normal subgroups.*
4) *$\Delta^+(G) = \{1\}$.*

Proof. We first prove that 1) $\implies$ 2). Since $Z(K[G])$ is commutative, we need to prove that there are no non-trivial zero divisors. Let $\alpha, \beta \in Z(K[G])$ be such that $\alpha\beta = 0$. Let $A = \alpha K[G]$ and $B = \beta K[G]$. Since both α and β are central, both A and B are ideals of $K[G]$. Since $AB = \{0\}$, it follows that either $A = \{0\}$ or $B = \{0\}$, as $K[G]$ is prime by assumption. Thus either $\alpha = 0$ or $\beta = 0$.

We now prove that 2) $\implies$ 3). Let N be a normal finite subgroup of G. By Lemma 11.1, $\widehat{N} = \sum_{x \in N} x$ is central in $K[G]$ and $\widehat{N}(\widehat{N} - |N|1) = 0$. Since $\widehat{N} \neq 0$ (recall that K has characteristic zero) and $Z(K[G])$ is a domain, $\widehat{N} = |N|1$, that is $N = \{1\}$.

Let us prove that 3) $\implies$ 4). Let $x \in \Delta^+(G)$. By Lemma 11.3, there exists a finite normal subgroup H of G that contains x. By assumption, H is trivial. Hence $x = 1$.

Finally, let us prove that 4) $\implies$ 1). Let A and B be ideals of $K[G]$ such that $AB = \{0\}$. Assume that $B \neq \{0\}$ and let $\beta \in B \setminus \{0\}$. If $\alpha \in A$, then, since

$$\alpha K[G]\beta \subseteq \alpha B \subseteq AB = \{0\},$$

Passman's lemma 4.7 implies that $\pi_{\Delta(G)}(\alpha)\pi_{\Delta(G)}(\beta) = \{0\}$. By assumption, $\Delta^+(G)$ is trivial. Thus $\Delta(G)$ is torsion-free. As $\Delta(\Delta(G)) = \Delta(G)$, it follows from Proposition 4.1 that $\Delta(G)$ is abelian. Therefore $K[\Delta(G)]$ has no zero divisors and therefore $\alpha = 0$. □

We now need to recall Hopkins–Levitzky's theorem. The theorem states that unitary left artinian rings are left noetherian.

Theorem 11.5 (Connel). *Let K be a field of characteristic zero. If G is a group, then $K[G]$ is left artinian if and only if G is finite.*

Proof. If G is finite, $K[G]$ is left artinian, as it is a finite-dimensional algebra.

Let us assume that $K[G]$ is left artinian. If $K[G]$ is prime, Wedderburn's theorem implies that $K[G]$ is simple and hence G is trivial (otherwise, $K[G]$ is not simple as the augmentation ideal is a non-zero ideal of $K[G]$).

Since $K[G]$ is left artinian, it is left noetherian by Hopkins–Levitzky's theorem. Thus $K[G]$ admits a composition series. We proceed by induction on the length of this composition series of $K[G]$. If the length is one, $\{0\}$ is the only ideal of $K[G]$ and hence the result follows as $K[G]$ is prime. If we assume the result holds for length n and $K[G]$ is not prime, then, Connel's theorem implies that G contains a finite non-trivial normal subgroup H. The canonical map $K[G] \to K[G/H]$ implies that $K[G/H]$ is left artinian and has length $< n$. By using the inductive hypothesis, G/H is a finite group. Since H is also finite, it follows that G is finite. □

§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.

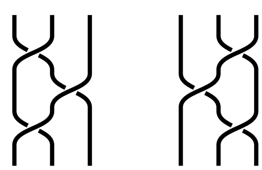

fig:braid

Figure 7.1: 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

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

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

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

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 7.2.

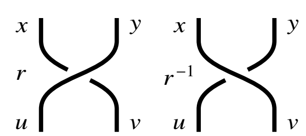

fig:square **Figure 7.2:** Any row or column determines the whole square.

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. Then (X,r), where $r(x,y) = (2x-y,x)$, is a solution.

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 $i(x) = x^{-1}$. □

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 $r(v,y^{-1}) = (u^{-1},x)$. □

§13. Radical rings and solutions

Let S be a non-unitary ring. Consider $S_1 = \mathbb{Z}\times S$ with the addition defined componentwise and multiplication

$$(k,a)(l,b) = (kl, kb+la+ab)$$

for all $k,l \in \mathbb{Z}$ and $a,b \in S$. Then S_1 is a ring and $(1,0)$ is its unit element. Furthermore, $\{0\}\times S$ is an ideal of S_1. Note that $\{0\}\times S \simeq S$ as non-unitary rings. Also note that if $(k,x) \in S_1$ is invertible, then $k \in \{-1,1\}$.

Definition 13.1. A non-unitary ring S is a (Jacobson) **radical ring** if it is isomorphic to the Jacobson radical of a unitary ring.

Let R be a ring. The (Jacobson) **radical** $J(R)$ of R is defined as the intersection of all maximal left ideals of R. One proves that $J(R)$ is an ideal of R. Moreover, $x \in J(R)$ if and only if $1+rx$ is invertible for all $r \in R$.

pro:radical **Proposition 13.2.** *Let S be a non-unitary ring. The following statements are equivalent.*

1) *S is a radical ring.*
2) *For all $a \in S$ there exists a unique $b \in S$ such that $a+b+ab = a+b+ba = 0$.*
3) *$S \simeq J(S_1)$.*

Proof. Let us first prove that 1) $\implies$ 2). Let R be a unitary ring such that $S \simeq J(R)$ and let $\psi\colon S \to R$ be an injective homomorphism of non-unitary rings $\psi(S) = J(R)$. Let $a \in S$. Since $1+\psi(a) \in R$ is invertible, there exists $c \in R$ such that

$$(1+\psi(a))(1+c) = (1+c)(1+\psi(a)) = 1.$$

Thus $c = -\psi(a)c - \psi(a) \in J(R)$. Hence there exists $b \in S$ such that $\psi(b) = c$. Therefore

$$a+b+ab = a+b+ba = 0.$$

It is an exercise to prove that b is unique.

We now prove that 2) $\implies$ 3). We first note that if $a \in S$, then there exists $b \in S$ such that $a+b+ab = a+b+ba = 0$. Thus every $(1,a) \in S_1$ is invertible, as

$$(1,a)(1,b) = (1,0) = (1,b)(1,a).$$

We claim that $J(S_1) = \{0\} \times S$. Let us prove that $J(S_1) \supseteq \{0\} \times S$. If $(k,a) \in J(S_1)$, then, in particular,

$$(1+3k, 3a) = (1,0) + (3,0)(k,a)$$

is invertible, which implies that either $1+3k = 1$ or $1+3k = -1$. Since $k \in \mathbb{Z}$, it follows that $k = 0$ and hence $(k,a) = (0,a) \in \{0\} \times S$. To prove that $J(S_1) \supseteq \{0\} \times S$ note that if $(0,x) \in \{0\} \times S$, then

$$(1,0) + (k,a)(0,x) = (1, kx + ax)$$

is invertible, as $kx + ax \in S$.

The implication 3) $\implies$ 1) is trivial. $\square$

Lecture 8

A **nil ring** is a non-unitary ring S such that every element of S is nilpotent. Every nil ring is a radical ring.

Example 13.3. $X\mathbb{C}[[X]]$ is a radical ring and it is not a nil ring.

Let S be a ring (unitary or non-unitary, it is not important here). Define on S the binary operation

$$(a,b) \mapsto a \circ b = a + b + ab$$

for all $a, b \in S$. Then $(S, \circ)$ is a monoid with neutral element 0. Note that S is a radical ring if and only if $(S, \circ)$ is a group. If $a \in S$ is invertible in the monoid $(S, \circ)$, we will denote by a' its inverse.

Example 13.4. For $n > 1$ let $A = \left\{ \frac{nx}{ny+1} : x, y \in \mathbb{Z} \right\} \subseteq \mathbb{Q}$. Note that A is a (non-unitary) subring of $\mathbb{Q}$. In fact, A is a radical ring. A straightforward computation shows that

$$\left(\frac{nx}{ny+1} \right)' = \frac{-nx}{n(x+y)+1}.$$

We now go back to study solutions to the YBE and discuss the intriguing interplay between radical rings and involutive solutions.

Definition 13.5. A solution (X, r) is said to be *involutive* if $r^2 = \mathrm{id}$.

Note that if (X, r) is an involutive solution, then

$$(x,y) = r^2(x,y) = r(\sigma_x(y), \tau_y(x)) = (\sigma_{\sigma_x(y)}\tau_y(x), \tau_{\tau_y(x)}\sigma_x(y)).$$

Hence

$$\tau_y(x) = \sigma^{-1}_{\sigma_x(y)}(x), \quad \sigma_x(y) = \tau^{-1}_{\tau_y(x)}(y) \tag{8.1}$$ eq:involutive

for all $x, y \in X$. Thus for involutive solutions it is enough to know $\{\sigma_x : x \in X\}$, as from this we obtain the set $\{\tau_x : x \in X\}$.

Example 13.6. Let X be a non-empty set and σ be a bijection on X. Then (X,r), where $r(x,y) = (\sigma(y),\sigma^{-1}(x))$, is an involutive solution.

We now present a very important family of involutive solutions.

thm:Rump **Theorem 13.7 (Rump).** *Let R be a radical ring. Then (R,r), where*

$$r(x,y) = (-x+x\circ y, (-x+x\circ y)'\circ x\circ y)$$

is an involutive solution.

The proposition can demonstrated using Theorem 12.13. We will prove a more general result later.

§14. Braces

By convention, an additive group A will be a (not necessarily abelian) group with a binary operation $(a,b)\mapsto a+b$. The identity of A will be denoted by 0 and the inverse of an element a will be denoted by $-a$.

Definition 14.1. A *brace* is a triple $(A,+,\circ)$, where $(A,+)$ and $(A,\circ)$ are (not necessarily abelian) groups and

$$a\circ(b+c) = (a\circ b)-a+(a\circ c) \tag{8.2}$$ eq:compatibility

holds for all $a,b,c\in A$. The groups $(A,+)$ and $(A,\circ)$ are respectively the *additive* and *multiplicative* group of the brace A.

We write a' to denote the inverse of a with respect to the circle operation $\circ$.

Our definition is that of left braces. Right braces are defined similarly, one needs to replace (8.2) by

$$(a+b)\circ c = a\circ c-c+b\circ c.$$

Definition 14.2. Let $\mathcal{X}$ be a family of groups. A brace A is said to be of $\mathcal{X}$-type if its additive group belongs to $\mathcal{X}$.

One particularly interesting family of braces is the family of *braces of abelian type*, that is braces with abelian additive group. In the literature, our braces are called *skew braces* and braces of abelian type are called *braces*.

exa:trivial **Example 14.3.** Let A be an additive group. Then A is a brace with $a\circ b = a+b$ for all $a,b\in A$. A brace $(A,+,\circ)$ such that $a\circ b = a+b$ for all $a,b\in A$ is said to be *trivial*. Similarly, the operation $a\circ b = b+a$ turns A into a brace.

exa:times **Example 14.4.** Let A and B be braces. Then $A\times B$ with

$$(a,b)+(a_1,b_1) = (a+a_1,b+b_1),\quad (a,b)\circ(a_1,b_1) = (a\circ a_1,b\circ b_1),$$

is a brace. This is the *direct product* of the braces A and B.

exa:sd **Example 14.5.** Let A and M be additive groups and let $\alpha\colon A \to \mathrm{Aut}(M)$ be a group homomorphism. Then $M \times A$ with

$$(x,a)+(y,b) = (x+y, a+b), \quad (x,a)\circ(y,b) = (x+\alpha_a(y), a+b)$$

is a brace. Similarly, $M \times A$ with

$$(x,a)+(y,b) = (x+\alpha_a(y), a+b), \quad (x,a)\circ(y,b) = (x+y, b+a)$$

is a brace.

exa:WX **Example 14.6.** Let A be an additive group and B and C be subgroups of A such that $B \cap C = \{0\}$ and $A = B+C$. In this case, one says that A admits an *exact factorization* through the subgroups B and C. Thus each $a \in A$ can be written in a unique way as $a = b+c$, for some $b \in B$ and $c \in C$. The map

$$B \times C \to A, \quad (b,c) \mapsto b-c,$$

is bijective. Using this map we transport the group structure of $B \times C$ into the set A. That is, for $a = b+c \in A$, where $b \in B$ and $c \in C$, and $a_1 \in A$, let

$$a \circ a_1 = b + a_1 + c.$$

Then $(A,\circ)$ is a group isomorphic to $B \times C$. Moreover, if $x, y \in A$, then

$$a\circ x - a + a\circ y = b+x+c-(b+c)+b+y+c = b+x+y+c = a\circ(x+y),$$

and therefore $(A,+,\circ)$ is a brace.

We now give concrete some examples of the previous construction.

exa:QR **Example 14.7.** Let n be a positive integer. The group $\mathbf{GL}_n(\mathbb{C})$ admits an exact factorization through the subgroups $U(n)$ and $T(n)$, where

$$U(n) = \{A \in \mathbf{GL}_n(\mathbb{C}) : AA^* = I\}$$

is the unitary group and $T(n)$ is the group of upper triangular matrices with positive diagonal entries. Therefore there exists a brace with additive group isomorphic to $\mathbf{GL}_n(\mathbb{C})$ and multiplicative group isomorphic to $U(n) \times T(n)$.

The following examples appeared in the theory of Hopf–Galois structures.

exa:a5a4c5 **Example 14.8.** The alternating simple group $\mathbb{A}_5$ admits an exact factorization through the subgroups $A = \langle (123), (12)(34) \rangle \simeq \mathbb{A}_4$ and $B = \langle (12345) \rangle \simeq C_5$. There exists a brace with additive group isomorphic to $\mathbb{A}_5$ and multiplicative group isomorphic to $\mathbb{A}_4 \times C_5$.

Let us review some basic properties of braces.

xca:0=1 **Exercise 14.9.** Let A be a brace. Then the following properties hold:

1) The neutral element of the additive group of A coincides with the neutral element of the multiplicative group of A. It will be denoted by 0.
2) $a \circ (-b+c) = a - (a \circ b) + (a \circ c)$, for all $a, b, c \in A$.
3) $a \circ (b-c) = (a \circ b) - (a \circ c) + a$, for all $a, b, c \in A$.

xca:lambda **Exercise 14.10.** Let A be a brace. For each $a \in A$, the map

$$\lambda_a \colon A \to A, \quad b \mapsto -a + (a \circ b),$$

is an automorphism of $(A, +)$. Moreover, the map $\lambda\colon (A, \circ) \to \operatorname{Aut}(A, +)$, $a \mapsto \lambda_a$, is a group homomorphism.

xca:mu **Exercise 14.11.** Let A be a brace. For each $a \in A$, the map

$$\mu_a \colon A \to A, \quad b \mapsto \lambda_b(a)' \circ b \circ a,$$

is bijective. Moreover, the map $\mu\colon (A, \circ) \to \mathbb{S}_A$, $a \mapsto \mu_a$, satisfies $\mu_b \circ \mu_a = \mu_{a\circ b}$, for all $a, b \in A$.

Let A be a brace. Exercise 14.10 implies that

$$a \circ b = a + \lambda_a(b), \qquad a + b = a \circ \lambda_a^{-1}(b), \qquad \lambda_a(a') = -a \tag{8.3}$$ eq:formulas

hold for $a, b \in A$. Moreover, if

$$a * b = \lambda_a(b) - b = -a + a \circ b - b,$$

then the following identities are easily verified:

$$a * (b+c) = a * b + b + a * c - b, \tag{8.4}$$
$$(a \circ b) * c = (a * (b * c)) + b * c + a * c. \tag{8.5}$$

Definition 14.12. A map $f\colon A \to B$ between two braces A and B is a *homomorphism of braces* if $f(x \circ y) = f(x) \circ f(y)$ and $f(x+y) = f(x) + f(y)$ for all $x, y \in A$. The *kernel* of f is

$$\ker f = \{a \in A : f(a) = 0\}.$$

A bijective homomorphism of braces is an isomorphism. An automorphism of a brace A is an isomorphism from the brace A to it self. Two braces A and B are isomorphic if there exist an isomorphism $f\colon A \to B$. We write $A \simeq B$ to denote that the braces A and B are isomorphic.

Definition 14.13. A brace A is said to be **two-sided** if

$$(a+b) \circ c = a \circ c - c + b \circ c \tag{8.6}$$ eq:right_compatibility

holds for all $a, b, c \in A$.

If A is a two-sided brace, then

$$a\circ(-b)=a-a\circ b+a,\qquad (-a)\circ b=b-a\circ b+b \tag{8.7}$$ eq:2sided

hold for all $a,b\in A$. The first equality holds for every brace and follows from the compatibility condition. The second equality follows from (8.6).

Example 14.14. Any brace with abelian multiplicative group is two-sided.

xca:2sided **Exercise 14.15.** Let A be a brace of abelian type such that $\lambda_a(a)=a$ for all $a\in A$. Prove that A is two-sided.

Two-sided braces of abelian type form an interesting family of non-unitary rings. Thus braces form a far reaching generalization of radical rings.

thm:radical **Theorem 14.16 (Rump).** *A brace of abelian type is two-sided if and only if it is a radical ring.*

Proof. Assume first that A is a two-sided brace of abelian type. Then $(A,+)$ is an abelian group. Let us prove that the operation

$$a*b=-a+a\circ b-b$$

turns A into a radical ring. Left distributivity follows from the compatibility condition:

$$a*(b+c)=-a+a\circ(b+c)-(b+c)=-a+a\circ b-a+a\circ c-c-b=a*b+a*c.$$

Similarly, since A is two-sided, one proves $(a+b)*c=a*c+b*c$. It remains to show that the operation $*$ is associative. On the one hand, using the first equality of (8.7) and the compatibility condition, we write

$$\begin{aligned}
a*(b*c)&=a*(-b+b\circ c-c)\\
&=-a+a\circ(-b+b\circ c-c)-(-b+b\circ c-c)\\
&=-a+a\circ(-b)-a+a\circ(b\circ c)-a+a\circ(-c)+c-b\circ c+b\\
&=a\circ(b\circ c)-a\circ b-a\circ c-b\circ c+a+b+c,
\end{aligned}$$

since the group $(A,+)$ is abelian. On the other hand, the second equality of (8.7) and Equality (8.6) imply that

$$\begin{aligned}
(a*b)*c=(-a+a\circ b-b)*c&=-(-a+a\circ b-b)+(-a+a\circ b-b)\circ c-c\\
&=b-a\circ b+a+(-a)\circ c-c+(a\circ b)\circ c-c+(-b)\circ c-c\\
&=(a\circ b)\circ c-a\circ b-a\circ c-b\circ c+a+b+c.
\end{aligned}$$

It then follows that the operation $*$ is associative.

Conversely, if A is a radical ring, say with ring multiplication $(a,b)\mapsto ab$, then $a\circ b=a+ab+b$ turns A into a two-sided brace of abelian type. In fact, since A is a radical ring, then $(A,+)$ is an abelian group and $(A,\circ)$ is a group. Moreover,

$$a \circ (b+c) = a + a(b+c) + (b+c) = a + ab + ac + b + c = a \circ b - a + a \circ c.$$

Similarly ones proves $(a+b) \circ c = a \circ c - c + b \circ c$. □

A natural question arises: Does one need radical rings? Surprisingly, radical rings are just the tip of the iceberg.

thm:YB **Theorem 14.17.** *Let A be a brace. Then (A,r), where*

$$r\colon A \times A \to A \times A, \quad r(x,y) = (-x + x \circ y, (-x + x \circ y)' \circ x \circ y),$$

is a solution to the YBE.

Proof. By Theorem 12.13, since $x \circ y = (-x + x \circ y) \circ ((-x + x \circ y)' \circ x \circ y)$ for all $x, y \in A$, we only need to check that $x \triangleright y = \lambda_x(y) = -x + x \circ y$ is a left action of $(A, \circ)$ on the set A and that $x \triangleleft y = \mu_y(x) = (-x + x \circ y)' \circ x \circ y$ is a right action of $(A, \circ)$ on the set A. For the left action we use Exercise 14.10 and for the right action we use Exercise 14.11. □

Exercise 14.18. Let A be a brace. Prove that

$$\mu_b(a) = \lambda^{-1}_{\lambda_a(b)}(-a \circ b + a + a \circ b).$$

In Theorem 14.17 it is possible to prove that the solution is involutive if and only if the additive group of the brace is abelian. We will prove a generalization of this result. For that purpose, we need a lemma.

lem:|r| **Lemma 14.19.** *Let A be a brace and r be its associated solution. Then*

$$\begin{aligned} r^{2n}(a,b) = (&-n(a \circ b) + a + n(a \circ b), \\ &(-n(a \circ b) + a + n(a \circ b))' \circ a \circ b), \end{aligned} \tag{8.8}$$
eq:r^2n

$$\begin{aligned} r^{2n+1}(a,b) = (&-n(a \circ b) - a + (n+1)(a \circ b), \\ &(-n(a \circ b) - a + (n+1)(a \circ b))' \circ a \circ b), \end{aligned} \tag{8.9}$$
eq:r^2n+1

for all $n \geq 0$. Moreover, the following statements hold:

1) $r^{2n} = \mathrm{id}$ *if and only if $a + nb = nb + a$ for all $a, b \in A$.*
2) $r^{2n+1} = \mathrm{id}$ *if and only if $\lambda_a(b) = n(a \circ b) + a - n(a \circ b)$ for all $a, b \in A$.*

Proof. First we shall prove (8.8) and (8.9) by induction on n. The case $n = 0$ is trivial for (8.8) and (8.9). Assume that the claim holds for some $n \geq 0$. By applying the map r to Equation (8.9) we obtain that

$$\begin{aligned} r^{2(n+1)}(a,b) &= r\,(-n(a \circ b) - a + (n+1)(a \circ b), \\ &\qquad (-n(a \circ b) - a + (n+1)(a \circ b))' \circ a \circ b) \\ &= (-(n+1)(a \circ b) + a + (n+1)(a \circ b), \\ &\qquad (-(n+1)(a \circ b) + a + (n+1)(a \circ b))' \circ a \circ b)\,. \end{aligned}$$

By applying r again to this equality, we get

$$\begin{aligned} r^{2(n+1)+1}(a,b) &= r\,(-(n+1)(a\circ b)+a+(n+1)(a\circ b), \\ &\qquad\qquad (-(n+1)(a\circ b)+a+(n+1)(a\circ b))'\circ a\circ b) \\ &= (-(n+1)(a\circ b)-a+(n+2)(a\circ b), \\ &\qquad\qquad (-(n+1)(a\circ b)-a+(n+2)(a\circ b))'\circ a\circ b)\,. \end{aligned}$$

Thus Equations (8.8) and (8.9) hold by induction. The other claims follow easily from Equations (8.8) and (8.9). □

Recall that the (minimal) *exponent* $\exp(G)$ of a finite group G is the least positive integer n such that $g^n = 1$ for all $g \in G$.

thm:|r|

Theorem 14.20. *Let A be a finite brace with more than one element and let K be the additive group of A. If r is the solution associated with A, then, as a permutation, r has order* $2\exp(K/Z(K))$.

Proof. Suppose that r has odd order $2n+1$. Since $r^{2n+1} = \mathrm{id}$, Lemma 14.19 implies that $-a+(n+1)(a\circ b) = n(a\circ b)+a$ for all $a,b \in A$. In particular, for $b = 0$, we get $a = 0$, for all $a \in A$, a contradiction. Therefore we may assume that the order of the permutation r is $2n$, where

$$n = \min\{k \in \mathbb{Z} : k > 0 \text{ and } kb+a = a+kb \;\text{ for all } a,b \in A\}.$$

Now one computes

$$\begin{aligned} n &= \min\{k \in \mathbb{Z} : k > 0 \text{ and } kb \in Z(G) \text{ for all } b \in A\} \\ &= \min\{k \in \mathbb{Z} : k > 0 \text{ and } k(b+Z(G)) = Z(G) \text{ for all } b \in A\} = \exp(G/Z(G)). \end{aligned}$$ □

An inmmediate consequence is the following result.

Corollary 14.21. *Let A be a finite brace and r be its associated solution. Then r is involutive if and only if A is of abelian type.*

§15. Ideals

Definition 15.1. Let A be a brace. A *subbrace* of A is a non-empty subset B of A such that $(B,+)$ is a subgroup of $(A,+)$ and $(B,\circ)$ is a subgroup of $(A,\circ)$.

Definition 15.2. Let A be a brace. A *left ideal* of A is a subgroup $(I,+)$ of $(A,+)$ such that $\lambda_a(I) \subseteq I$ for all $a \in A$, i.e. $\lambda_a(x) \in I$ for all $a \in A$ and $x \in I$. A *strong left ideal* of A is a left ideal I of A such that $(I,+)$ is a normal subgroup of $(A,+)$.

Example 15.3. Let A be a brace and I be a characteristic subgroup of the additive group of A. Then I is a left ideal of A.

Recall that two-sided braces of abelian type are equivalent to radical rings. One can prove that under this equivalence, (left) ideals of the radical ring correspond to (left) ideals of the associated brace.

Proposition 15.4. *A left ideal I of a brace A is a subbrace of A.*

Proof. We need to prove that $(I,\circ)$ is a subgroup of $(A,\circ)$. Clearly I is non-empty, as it is an additive subgroup of A. If $x,y\in I$, then $x\circ y=x+\lambda_x(y)\in I+I\subseteq I$ and $x'=-\lambda_{x'}(x)\in I$. □

Example 15.5. Let A be a brace. Then

$$\mathrm{Fix}(A)=\{a\in A:\lambda_x(a)=a\text{ for all }x\in A\}$$

is a left ideal of A.

Definition 15.6. An *ideal* of a brace A is a strong left ideal I of A such that $(I,\circ)$ is a normal subgroup of $(A,\circ)$.

In general

$$\{\text{subbraces}\}\supsetneq\{\text{left ideals}\}\supsetneq\{\text{strong left ideals}\}\supsetneq\{\text{ideals}\}.$$

For example, $\mathrm{Fix}(A)$ is not a strong left ideal of A.

Example 15.7. Consider the semidirect product $A=\mathbb{Z}/(3)\rtimes\mathbb{Z}/(2)$ of the trivial braces $\mathbb{Z}/(3)$ and $\mathbb{Z}/(2)$ via the non-trivial action of $\mathbb{Z}/(2)$ over $\mathbb{Z}/(3)$. Then

$$\lambda_{(x,y)}(a,b)=-(x,y)+(x,y)\circ(a,b)=-(x,y)+(x+(-1)^y a,y+b)=((-1)^y a,b).$$

Then $\mathrm{Fix}(A)=\{(0,0),(0,1)\}$ is not a normal subgroup of $(A,+)$ and hence $\mathrm{Fix}(A)$ is not a strong left ideal of A.

Example 15.8. Let $f\colon A\to B$ be a homomorphism of braces. Then $\ker f$ is an ideal of A.

If X and Y are subsets of a brace A, $X*Y$ is defined as the subgroup of $(A,+)$ generated by elements of the form $x*y$, $x\in X$ and $y\in Y$, i.e.

$$X*Y=\langle x*y:x\in X,y\in Y\rangle_+.$$

pro:A*I **Proposition 15.9.** *Let A be a brace. A subgroup I of $(A,+)$ is a left ideal of A if and only if $A*I\subseteq I$.*

Proof. Let $a\in A$ and $x\in I$. If I is a left ideal, then $a*x=\lambda_a(x)-x\in I$. Conversely, if $A*I\subseteq I$, then $\lambda_a(x)=a*x+x\in I$. □

pro:I*A **Proposition 15.10.** *Let A be a brace. A normal subgroup I of $(A,+)$ is an ideal of A if and only $\lambda_a(I)\subseteq I$, for all $a\in A$, and $I*A\subseteq I$.*

Proof. Let $x \in I$ and $a \in A$. Assume first that I is invariant under the action of λ and that $I * A \subseteq I$. Then

$$\begin{aligned} a \circ x \circ a' &= a + \lambda_a(x \circ a') \\ &= a + \lambda_a(x + \lambda_x(a')) = a + \lambda_a(x) + \lambda_a \lambda_x(a') + a - a \\ &= a + \lambda_a(x + \lambda_x(a') - a') - a = a + \lambda_a(x + x * a') - a \in I, \end{aligned} \tag{8.10}$$

eq:trick:I*A

and hence I is an ideal.

Conversely, assume that I is an ideal. Then $I * A \subseteq I$ since

$$\begin{aligned} x * a &= -x + x \circ a - a \\ &= -x + a \circ (a' \circ x \circ a) - a = -x + a + \lambda_a(a' \circ x \circ a) - a \in I. \end{aligned}$$ □

Let I and J be ideals of a brace A. Then $I \cap J$ is an ideal of A. The sum $I + J$ of I and J is defined as the additive subgroup of A generated by all the elements of the form $u + v$, $u \in I$ and $v \in J$.

Proposition 15.11. *Let A be a brace and let I and J be ideals of A. Then $I + J$ is an ideal of A.*

Proof. Since I and J are normal subgroups of A, we have that

$$I + J = \{u + v \mid u \in I,\ v \in J\}.$$

First note that $I + J$ is a normal subgroup of $(A, +)$ since

$$a + (u + v) - a = (a + u - a) + (a + v - a) \in I + J$$

for all $u \in I$, $v \in J$ and $a \in A$. Let $a \in A$, $u \in I$ and $v \in J$. Then $\lambda_a(u + v) = \lambda_a(u) + \lambda_a(v) \in I + J$ and hence it follows that $\lambda_a(I + J) \subseteq I + J$. Moreover, by Propositions 15.9 and 15.10,

$$(u + v) * a = (u \circ \lambda_u^{-1}(v)) * a = u * (\lambda_u^{-1}(v) * a) + \lambda_u^{-1}(v) * a + u * a \in I + J.$$

Hence $(I + J) * A \subseteq I + J$. Therefore the result follows by Proposition 15.10. □

Definition 15.12. Let A be a brace. The subset $\operatorname{Soc}(A) = \ker \lambda \cap Z(A, +)$ is the *socle* of A.

We will use the following exercise several times.

xca:socle

Exercise 15.13. Let A be a brace and $a \in \operatorname{Soc}(A)$. Prove that

$$b + b \circ a = b \circ a + b \quad \text{and} \quad \lambda_b(a) = b \circ a \circ b'$$

hold for all $b \in A$.

xca:Bachiller1

Exercise 15.14. Prove that the socle of a brace A is the kernel of the group homomorphism $(A, \circ) \to \operatorname{Aut}(A, +) \times \mathbb{S}_A$, $a \mapsto (\lambda_a, \mu_a^{-1})$.

xca:Bachiller2

Exercise 15.15. Prove that the socle of a brace A is the kernel of the group homomorphism

$$(A,\circ) \to \operatorname{Aut}(A,+) \times \operatorname{Aut}(A,+), \quad a \mapsto (\lambda_a, \xi_a),$$

where $\xi_a(b) = a + \lambda_a(b) - a$.

pro:socle

Proposition 15.16. *Let A be a brace. Then* $\operatorname{Soc}(A)$ *is an ideal of A.*

Proof. Clearly $0 \in \operatorname{Soc}(A)$, since λ is a group homomorphism. Let $a, b \in \operatorname{Soc}(A)$ and $c \in A$. Since $b \circ (-b) = b + (-b) = 0$, it follows that $b' = -b \in \operatorname{Soc}(A)$. The calculation

$$\lambda_{a-b}(c) = \lambda_{a \circ b'}(c) = \lambda_a \lambda_b^{-1}(c) = c,$$

implies that $a - b \in \ker \lambda$. Since $a - b \in Z(A,+)$, it follows that $(\operatorname{Soc}(A),+)$ is a normal subgroup of $(A,+)$.

For each $d \in A$, $a + c' \circ d = c' \circ d + a$. By Exercise 15.13, we have

$$\begin{aligned} d + \lambda_c(a) &= d - c + c \circ a = c \circ (c' \circ d + a) \\ &= c \circ (a + c' \circ d) = c \circ a - c + d = -c + c \circ a + d = \lambda_c(a) + d, \end{aligned}$$

that is $\lambda_c(a)$ is central in $(A,+)$. Moreover, again by Exercise 15.13,

$$\begin{aligned} \lambda_c(a) + d &= -c + c \circ a + d = c \circ a - c + d \\ &= c \circ (a + (c' \circ d)) = c \circ a \circ c' \circ d = \lambda_c(a) \circ d \end{aligned}$$

and hence

$$\lambda_{\lambda_c(a)}(d) = -\lambda_c(a) + \lambda_c(a) \circ d = -\lambda_c(a) + \lambda_c(a) + d = d.$$

Therefore $\operatorname{Soc}(A)$ is a strong left ideal of A. In fact, $\operatorname{Soc}(A)$ is an ideal of A, as $c \circ a \circ c' = \lambda_c(a) \in \operatorname{Soc}(A)$. □

As a corollary we obtain that the socle of a brace A is a trivial brace of abelian type.

pro:soc_kernels

Proposition 15.17. *Let A be a brace. Then* $\operatorname{Soc}(A) = \ker \lambda \cap \ker \mu$.

Proof. Let $a \in \operatorname{Soc}(A)$ and $b \in A$. Then $\lambda_a = \mathrm{id}$ and $a \in Z(A,+)$. By Exercise 15.13,

$$\mu_a(b) = \lambda_b(a)' \circ b \circ a = (b \circ a \circ b')' \circ b \circ a = b.$$

Thus $a \in \ker \lambda \cap \ker \mu$.

Conversely, let $a \in \ker \lambda \cap \ker \mu$ and $b \in A$. Then $b' = \mu_a(b') = \lambda_{b'}(a)' \circ b' \circ a$, so $\lambda_{b'}(a) = b' \circ a \circ b$. Now

$$b + a = b \circ \lambda_b^{-1}(a) = b \circ \lambda_{b'}(a) = b \circ b' \circ a \circ b = a \circ b = a + \lambda_a(b) = a + b$$

implies that $a \in \operatorname{Soc}(A)$. □

Definition 15.18. Let A be a brace. The *annihilator* of A is defined as the set $\operatorname{Ann}(A) = \operatorname{Soc}(A) \cap Z(A, \circ)$.

Note that $\operatorname{Ann}(A) \subseteq \operatorname{Fix}(A)$.

Proposition 15.19. *The annihilator of a brace A is an ideal of A.*

Proof. Let $x, y \in \operatorname{Ann}(A)$. Note that $x - y = x \circ y' \in Z(A, \circ)$. Hence $\operatorname{Ann}(A)$ is a subbrace of A. Since $\operatorname{Ann}(A) \subseteq Z(A,+) \cap Z(A,\circ)$, we only need to note that $\lambda_a(x) = x \in \operatorname{Ann}(A)$, for all $a \in A$. □

If A is a brace and I is an ideal of A, then $a + I = a \circ I$ for all $a \in A$. Indeed, $a \circ x = a + \lambda_a(x) \in a + I$ and $a + x = a \circ \lambda_a^{-1}(x) = a \circ \lambda_{a'}(x) \in a \circ I$ for all $a \in A$ and $x \in I$. This allows us to prove that there exists a unique brace structure over A/I such that the map

$$\pi\colon A \to A/I, \quad a \mapsto a + I = a \circ I,$$

is a homomorphism of braces. The brace A/I is the **quotient brace** of A modulo I.

xca:iso1 **Exercise 15.20.** Let A and B be braces and $f\colon A \to B$ be a homomorphism. Prove that $A/\ker f \simeq f(A)$.

xca:iso2 **Exercise 15.21.** Let A be a brace and let B be a subbrace of A. Prove that if I is an ideal of A, then $B \circ I$ is a subbrace of A, $B \cap I$ is an ideal of B and $(B \circ I)/I \simeq B/(B \cap I)$.

xca:iso3 **Exercise 15.22.** Let A be a brace and I and J be ideals of A. Prove that if $I \subseteq J$, then $A/J \simeq (A/I)/(J/I)$.

xca:correspondence **Exercise 15.23.** Let A be a brace and let I be an ideal of A. Prove that there is a bijective correspondence between (left) ideals of A containing I and (left) ideals of A/I.

Lecture 9

§16. Braces and 1-cocycles

Let K and Q be groups. An *extension* of K by Q is a short exact sequence of group homomorphisms

$$1 \longrightarrow K \xrightarrow{f} G \xrightarrow{g} Q \longrightarrow 1$$

This means that f is injective, g is surjective and $\ker g = \operatorname{im} f$. Note that in this case, K is isomorphic to $f(K)$, which is a normal subgroup of G and $G/f(K) \simeq Q$. We also say that G is an extension of K by Q.

Example 16.1. C_6 and $\mathbb{S}_3$ are both extensions of C_3 by C_2.

Example 16.2. C_6 is an extension of C_2 by C_3.

Example 16.3. The direct product $K \times Q$ of the groups K and Q is an extension of K by Q and an extension of Q by K.

Example 16.4. Let G be an extension of K by Q. If L is a subgroup of G containing K, then L is an extension of K by L/K.

Let $E:\ 1 \longrightarrow K \longrightarrow G \xrightarrow{p} Q \longrightarrow 1$ be an extension of groups. A *lifting* of E is a map $\ell\colon Q \to G$ such that $p(\ell(x)) = x$, for all $x \in Q$.

An extension E *splits* if there is a lifting of E that it is a group homomorphism.

xca:lifting

Exercise 16.5. Let $E:\ 1 \longrightarrow K \longrightarrow G \xrightarrow{p} Q \longrightarrow 1$ be an extension.

1) If $\ell\colon Q \to G$ is a lifting, then $\ell(Q)$ is a transversal of $\ker p$ in G.
2) Each transversal of $\ker p$ in G induces a lifting $\ell\colon Q \to G$.
3) If $\ell\colon Q \to G$ is a lifting, then $\ell(xy)\ker p = \ell(x)\ell(y)\ker p$.

Let Q and K be groups. Assume that Q acts by automorphisms on K, that is there is a group homomorphism $\alpha\colon Q \to \mathrm{Aut}(k)$. We write $\alpha_x = \alpha(x)$, for all $x \in Q$. A map $\varphi\colon Q \to K$ is said to be a 1-*cocycle* (or a derivation) if

$$\varphi(xy) = \varphi(x)\alpha_x(\varphi(y)),$$

for all $x, y \in Q$. The set of 1-cocycles $Q \to K$ is defined as

$$\mathrm{Der}(Q,K) = Z^1(Q,K) = \{\delta\colon Q \to K : \delta \text{ is 1-cocycle}\}.$$

Example 16.6. Let K and Q be groups. Let $\alpha\colon Q \to \mathrm{Aut}(K)$ be a group homomorphism. For each $k \in K$, the map $\delta_k : Q \to K$, $x \mapsto \delta_k(x) = k\alpha_x(k)^{-1}$, is a derivation. One typically writes $\delta_k(x) = [k,x]$.

xca:1cocycle

Exercise 16.7. Let $\varphi\colon Q \to K$ be a 1-cocycle.

1) $\varphi(1) = 1$.
2) $\varphi(y^{-1}) = (y^{-1}\cdot\varphi(y))^{-1} = y^{-1}\cdot\varphi(y)^{-1}$.
3) The set $\ker\varphi = \{x \in Q : \varphi(x) = 1\}$ is a subgroup of Q.

A subgroup K of a group G admits a *complement* Q if G admits an exact factorization through K and Q, i.e. $G = KQ$ with $K \cap Q = \{1\}$. A classical example is the (inner) semidirect product $G = K \rtimes Q$, where K is a normal subgroup of G and Q is a subgroup of G such that $K \cap Q = \{1\}$.

Let K and Q be groups. Let $\alpha\colon Q \to \mathrm{Aut}(K)$, $x \mapsto \alpha_x$ be a group homomorphism. Consider the set $K \times Q$. We define a multiplication on this set by

$$(k_1, q_1)(k_2, q_2) = (k_1\alpha_{q_1}(k_2), q_1q_2),$$

for all $k_1, k_2 \in K$ and $q_1, q_2 \in Q$. Then $K \times Q$ with this multiplication is a group, called the semidirect product of K by Q via α, and denoted by $K \rtimes_\alpha Q$. Note that $K \times \{1\}$ is a normal subgroup of $K \rtimes_\alpha Q$, and $\{1\} \times Q$ is a subgroup of $K \rtimes_\alpha Q$. Thus $K \rtimes_\alpha Q$ is the inner semidirect product of $K \times \{1\}$ by $\{1\} \times Q$. Since $K \simeq K \times \{1\}$ and $Q \simeq \{1\} \times Q$, we identify these groups, i. e. $k \equiv (k,1)$ and $q \equiv (1,q)$ for all $k \in K$ and $q \in Q$. Note that

$$qkq^{-1} \equiv (1,q)(k,1)(1,q^{-1}) = (\alpha_q(k), q)(1,q^{-1}) = (\alpha_q(k),1) = \alpha_q(k)$$

for all $k \in K$ and $q \in Q$.

thm:complements

Theorem 16.8. *Let Q and K be groups and let $\alpha\colon Q \to \mathrm{Aut}(K)$ be a group homomorphism. Then there exists a bijective correspondence*

$$\{\textit{complements of } K \textit{ in } K \rtimes Q\} \leftrightarrow \mathrm{Der}(Q,K).$$

Proof. Let C be the set of complements of K in $K \rtimes Q$. Since Q acts by conjugation on K, it follows that $\delta \in \mathrm{Der}(Q,K)$ if and only if $\delta(xy) = \delta(x)x\delta(y)x^{-1}$ for all $x, y \in Q$. In this case, one obtains that $\delta(1) = 1$ and $\delta(x^{-1}) = x^{-1}\delta(x)^{-1}x$.

Let $C \in \mathcal{C}$. If $x \in Q$, then there exist unique elements $k \in K$ and $c \in C$ such that $x = k^{-1}c$. Hence the map $\delta_C \colon Q \to K$, $x \mapsto k$, is well-defined and $\delta_C(x)x = c \in C$.

We claim that $\delta_C \in \operatorname{Der}(Q,K)$. If $x, x_1 \in Q$, we write $x = k^{-1}c$ and $x_1 = k_1^{-1}c_1$ for $k, k_1 \in K$ and $c, c_1 \in C$. Since K is a normal subgroup of the semidirect product $K \rtimes Q$, we can write xx_1 as $xx_1 = k_2c_2$, where $k_2 = k^{-1}(ck_1^{-1}c^{-1}) \in K$, $c_2 = cc_1 \in C$. Thus $\delta_C(xx_1)xx_1 = cc_1 = \delta_C(x)x\delta_C(x_1)x_1$ implies that $\delta_C(xx_1) = \delta_C(x)x\delta_C(x_1)x^{-1}$. So there is a map $F \colon \mathcal{C} \to \operatorname{Der}(Q,K)$, $F(C) = \delta_C$.

We now construct a map $G \colon \operatorname{Der}(Q,K) \to \mathcal{C}$. For each $\delta \in \operatorname{Der}(Q,K)$ we find a complement Δ of K in $K \rtimes Q$. Let $\Delta = \{\delta(x)x : x \in Q\}$. We claim that Δ is a subgroup of $K \rtimes Q$. Since $\delta(1) = 1$, $1 \in \Delta$. If $x, y \in Q$, then

$$\delta(x)x\delta(y)y = \delta(x)x\delta(y)x^{-1}xy = \delta(xy)xy \in \Delta.$$

Finally, if $x \in Q$, then

$$(\delta(x)x)^{-1} = x^{-1}\delta(x)^{-1}xx^{-1} = \delta(x^{-1})x^{-1} \in \Delta.$$

Thus Δ is a subgroup of $K \rtimes Q$. We claim that $\Delta \cap K = \{1\}$. If $x \in Q$ is such that $\delta(x)x \in K$, then since $\delta(x) \in K$, it follows that $x \in K \cap Q = \{1\}$. If $g \in G$, then there are unique $k \in K$ and $x \in Q$ such that $g = kx$. We write $g = k\delta(x)^{-1}\delta(x)x$. Since $k\delta(x)^{-1} \in K$ and $\delta(x)x \in \Delta$, we conclude that $G = K\Delta$. Thus there is a well-defined map $G \colon \operatorname{Der}(Q,K) \to \mathcal{C}$, $G(\delta) = \Delta$.

We claim that $G \circ F = \mathrm{id}_{\mathcal{C}}$. Let $C \in \mathcal{C}$. Then

$$G(F(C)) = G(\delta_C) = \{\delta_C(x)x : x \in Q\} = C,$$

by construction. (We know that $\delta_C(x)x \in C$. Conversely, if $c \in C$, we write $c = kx$ for unique elements $k \in K$ and $x \in Q$. Thus $x = k^{-1}c$ and hence $c = \delta_c(x)x$.)

Finally, we prove that $F \circ G = \mathrm{id}_{\operatorname{Der}(Q,K)}$. Let $\delta \in \operatorname{Der}(Q,K)$. Then

$$F(G(\delta)) = F(\Delta) = \delta_\Delta.$$

Finally, we need to show that $\delta_\Delta = \delta$. Let $x \in Q$. There exists $\delta(y)y \in \Delta$ for some $y \in Q$ such that $x = k^{-1}\delta(y)y$. Thus $\delta_\Delta(x)x = \delta(y)y$ and hence $x = y$ and $\delta_\Delta(x) = \delta(y)$ by the uniqueness. Therefore, $\delta_\Delta = \delta$, and the result follows. $\square$

Let K and Q be groups and let $\alpha \colon Q \to \operatorname{Aut}(K)$ be a group homomorphism. A derivation $\delta \in \operatorname{Der}(Q,K)$ is said to be *inner* if there exists $k \in K$ such that $\delta(x) = [k,x]$ for all $x \in Q$. The set of *inner derivations* will be denoted by

$$\operatorname{Inn}(Q,K) = B^1(Q,K) = \{\delta \in \operatorname{Der}(Q,K) : \delta \text{ is inner}\}.$$

An inner derivation is also called a 1-*coboundary*.

theorem:Sysak

Theorem 16.9 (Sysak). *Let K and Q be groups and let $\alpha \colon Q \to \operatorname{Aut}(K)$ be a group homomorphism. Let $\delta \in \operatorname{Der}(Q,K)$.*

1) *$\Delta = \{\delta(x)x : x \in Q\}$ is a complement of K in $K \rtimes Q$.*

2) *$\delta \in \mathrm{Inn}(Q,K)$ if and only if $\Delta = kQk^{-1}$ for some $k \in K$.*
3) *$\ker\delta = Q \cap \Delta$.*
4) *δ is surjective if and only if $K \rtimes Q = \Delta Q$.*

Proof. In the proof of Theorem 16.8 we found that Δ is a complement of K in $K \rtimes Q$.

Let us prove the second statement. If δ is inner, then there exists $k \in K$ such that $\delta(x) = [k,x] = kxk^{-1}x^{-1}$ for all $x \in Q$. Since $\delta(x)x = kxk^{-1}$ for all $x \in Q$, $\Delta = kQk^{-1}$. Conversely, if there exists $k \in K$ such that $\Delta = kQk^{-1}$, for each $x \in Q$ there exists $y \in Q$ such that $\delta(x)x = kyk^{-1}$. Since $[k,y] = kyk^{-1}y^{-1} \in K$, $\delta(x) \in K$ and $\delta(x)x = [k,y]y \in KQ$, we conclude that $x = y$ and hence $\delta(x) = [k,x]$.

Let us prove the third statement. If $x \in Q$ is such that $\delta(x)x = y \in Q$, then

$$\delta(x) = yx^{-1} \in K \cap Q = \{1\}.$$

Conversely, if $x \in Q$ is such that $\delta(x) = 1$, then $x = \delta(x)x \in Q \cap \Delta$.

Finally we prove the fourth statement. If δ is surjective, then for each $k \in K$ there exits $y \in Q$ such that $\delta(y) = k$. Thus $K \rtimes Q \subseteq \Delta Q$, as

$$kx = \delta(y)x = (\delta(y)y)y^{-1}x \in \Delta Q.$$

Since Δ and Q are subgroups of $K \rtimes Q$, we have that $\Delta Q \subseteq K \rtimes Q$, and therefore $\Delta Q = K \rtimes Q$. Conversely, if $k \in K$ and $x \in Q$ there exist $y, z \in Q$ such that $kx = \delta(y)yz$. Then it follows that $k = \delta(y)$. □

xca:ker1cocycle **Exercise 16.10.** Let $\delta \in \mathrm{Der}(Q,K)$.

1) Prove that δ is injective if and only if $\ker\delta = \{1\}$.
2) Prove that if δ is bijective, then K admits a complement Δ in $K \rtimes Q$ such that $K \rtimes Q = K \rtimes \Delta = \Delta Q$ and $Q \cap \Delta = \{1\}$.

A group G admits a *triple factorization* if there are subgroups A, B and M such that $G = MA = MB = AB$ and $A \cap M = B \cap M = \{1\}$. The following result is an immediate consequence of Sysak's theorem.

Corollary 16.11. *If the group Q acts by automorphisms on K and $\delta \in \mathrm{Der}(Q,K)$ is surjective, then $G = K \rtimes Q$ admits a triple factorization.*

Let A be an additive group (note that we do not assume that an additive group is abelian) and G be a group and let $G \times A \to A$, $(g,a) \mapsto g \cdot a$, be a left action of G on A by automorphisms. This means that the action of G on A satisfies $g \cdot (a+b) = g \cdot a + g \cdot b$ for all $g \in G$ and $a, b \in A$. A *bijective* 1*-cocyle* is a bijective map $\pi \colon G \to A$ such that

$$\pi(gh) = \pi(g) + g \cdot \pi(h) \tag{9.1}$$ eq:1cocycle

for all $g, h \in G$. To simplify the notation we just say that the pair (G,π) is a bijective 1-cocycle with values on A.

thm:1cocycle

Theorem 16.12. *Let A be an additive group. There exists a bijective correspondence*

$$\{\textit{bijective 1-cocycles with values on } A\} \leftrightarrow \{\textit{braces with additive group } A\}$$

Proof. Consider on A a second group structure given by

$$a \circ b = \pi(\pi^{-1}(a)\pi^{-1}(b)) = a + \pi^{-1}(a) \cdot b$$

for all $a, b \in A$. Since G acts on A by automorphisms,

$$\begin{aligned} a \circ (b+c) &= \pi(\pi^{-1}(a)\pi^{-1}(b+c)) = a + \pi^{-1}(a) \cdot (b+c) \\ &= a + \pi^{-1}(a) \cdot b + \pi^{-1}(a) \cdot c = a \circ b - a + a \circ c \end{aligned}$$

holds for all $a, b, c \in A$.

Conversely, assume that the additive group A has a brace structure. Let G be the multiplicative group of A and $\pi = \mathrm{id}$. By Exercise 14.10, $a \mapsto \lambda_a$ is a group homomorphism from G to $\mathrm{Aut}(A,+)$ and hence G acts on A by automorphisms. Then (9.1) holds and therefore $\pi\colon G \to A$ is a bijective 1-cocycle. □

The construction of the previous theorem is functorial.

xca:1cocycle

Exercise 16.13. Let $\pi\colon G \to A$ and $\eta\colon H \to B$ be bijective 1-cocycles. A *homorphism* between these bijective 1-cocycles is a pair (f, g) of group homomorphisms $f\colon G \to H$, $g\colon A \to B$ such that

$$\begin{aligned} &\eta f = g\pi, \\ &g(h \cdot a) = f(h) \cdot g(a), \qquad\qquad a \in A,\ h \in G. \end{aligned}$$

Bijective 1-cocycles and homomorphisms form a category. For a given additive group A the full subcategory of the category of bijective 1-cocycles with objects $\pi\colon G \to A$ is equivalent to the full subcategory of the category of braces with additive group A.

exa:d8q8

Example 16.14. Let

$$D_4 = \langle r, s : r^4 = s^2 = 1, srs = r^{-1} \rangle$$

be the dihedral group of eight elements and let

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$$

be the quaternion group of eight elements. Let $\pi : Q_8 \to D_4$ be given by

$$\begin{array}{llll} 1 \mapsto 1, & -1 \mapsto r^2, & -k \mapsto r^3 s, & k \mapsto rs, \\ i \mapsto s, & -i \mapsto r^2 s, & j \mapsto r^3, & -j \mapsto r. \end{array}$$

Since π is bijective, a straightforward calculation shows that D_4 with

$$x + y = xy, \quad x \circ y = \pi(\pi^{-1}(x)\pi^{-1}(y))$$

is a two-sided brace with additive group isomorphic to D_4 and multiplicative group isomorphic to Q_8.

Lecture 10

§17. Braces and regular subgroups

For an additive group A, the **holomorph** of A is the semidirect product

$$\operatorname{Hol}(A) = A \rtimes \operatorname{Aut}(A).$$

This means that the operation is

$$(a,f)(b,g) = (a+f(b), f\circ g), \quad a,b\in A, \quad f,g\in\operatorname{Aut}(A).$$

Every subgroup G of $\operatorname{Hol}(A)$ acts on A by

$$(x,f)\cdot a = \pi_1((x,f)(a,\mathrm{id})) = \pi_1(x+f(a),f) = x+f(a), \quad a,x\in A, \quad f\in\operatorname{Aut}(A),$$

where $\pi_1\colon \operatorname{Hol}(A)\to A$, $(a,f)\mapsto a$.

Exercise 17.1. The group $\operatorname{Hol}(A)$ acts transitively on A and the stabilizer $a\in A$ is isomorphic to $\operatorname{Aut}(A)$.

A subgroup G of $\operatorname{Hol}(A)$ is said to be *regular* if its acts regularly on A, this means that given $a,b\in A$ there exists a unique $(x,f)\in G$ such that

$$b = (x,f)\cdot a = x+f(a).$$

xca:bijective **Exercise 17.2.** Prove that if G is a regular subgroup of $\operatorname{Hol}(A)$, then $\pi_1\colon G\to A$ is bijective.

Now we establish an important connection between braces and regular subgroups.

thm:regular **Theorem 17.3.** *If A is a brace, then $\Delta = \{(a,\lambda_a) : a\in A\}$ is a regular subgroup of* $\operatorname{Hol}(A,+)$. *Conversely, if A is an additive group and G is a regular subgroup of* $\operatorname{Hol}(A)$*, then A is a brace with*

$$a\circ b = a+f(b),$$

where $(\pi_1|_G)^{-1}(a) = (a, f) \in G$.

Proof. Assume first that A is a brace. Using (8.3) and that λ is a group homomorphism, it follows that $\Delta = \{(a, \lambda_a) : a \in A\}$ is a subgroup of $\mathrm{Hol}(A, +)$, as

$$(a, \lambda_a)^{-1} = (\lambda_a^{-1}(-a), \lambda_a^{-1}) = (a', \lambda_{a'}) \in \Delta,$$
$$(a, \lambda_a)(b, \lambda_b) = (a + \lambda_a(b), \lambda_a \circ \lambda_b) = (a \circ b, \lambda_{a \circ b}) \in \Delta.$$

To see that Δ is a regular subgroup, note that $(c, \lambda_c) \cdot a = b$ implies that $c = b \circ a'$, as $(A, \circ)$ is a group.

Assume now that A is an additive group and that G is a regular subgroup of $\mathrm{Hol}(A)$. By Exercise 17.2, the restriction $\pi_1|_G$ is bijective. Use the bijection $\pi_1|_G$ to transport the operation of G into A:

$$a \circ b = \pi_1|_G\left((\pi_1|_G)^{-1}(a)(\pi_1|_G)^{-1}(b)\right) = a + f(b),$$

where $a, b \in A$ and $(\pi_1|_G)^{-1}(a) = (a, f) \in G$. Then $(A, \circ)$ is a group isomorphic to G and moreover A is a brace, as

$$\begin{aligned} a \circ (b + c) &= a + f(b + c) = a + f(b) + f(c) \\ &= a + f(b) - a + a + f(c) = a \circ b - a + a \circ c \end{aligned}$$

holds for all $a, b, c \in A$. □

lem:BNY

Lemma 17.4. *Let A be a group. If H and K are conjugate regular subgroups of* $\mathrm{Hol}(A)$*, then H and K are conjugate by an automorphism of A.*

Proof. Assume that H and K are conjugate in $\mathrm{Hol}(A)$. Let $(b, g) \in \mathrm{Hol}(A)$ be such that $(b, g)^{-1} H (b, g) = K$. Since $b \in A$, the regularity of H implies that there exists $(a, f) \in H$ such that $a + f(b) = 0$. Since $(a, f) \in H$,

$$\begin{aligned} K = (b, g)^{-1} H (b, g) &= (b, g)^{-1} (a, f)^{-1} H (a, f)(b, g) \\ &= (0, f \circ g)^{-1} H (0, f \circ g) = (f \circ g)^{-1} H (f \circ g). \end{aligned}$$ □

pro:regular

Proposition 17.5. *Let A be an additive group. There exists a bijective correspondence between isomorphism classes of brace structures with additive group A and conjugacy classes of regular subgroups of* $\mathrm{Hol}(A)$.

Proof. Assume that the additive group A has two isomorphic brace structures given by $(a, b) \mapsto a \circ b$ and $(a, b) \mapsto a \times b$. Let $f \colon A \to A$ be a bijective map such that $f(a + b) = f(a) + f(b)$ and $f(a \circ b) = f(a) \times f(b)$ for all $a, b \in A$. We claim that the regular subgroups $\{(a, \lambda_a) : a \in A\}$ and $\{(a, \mu_a) : a \in A\}$, where $\lambda_a(b) = -a + a \circ b$ and $\mu_a(b) = -a + a \times b$, are conjugate. Since f is an isomorphism of braces,

$$f \circ \lambda_a \circ f^{-1} = \mu_{f(a)}$$

for all $a \in A$. This implies that $(0, f)(a, \lambda_a)(0, f)^{-1} = (f(a), \mu_{f(a)})$ for all $a \in A$ and hence and the first claim follows.

Conversely, let H and K be conjugate regular subgroups of $\mathrm{Hol}(A)$. Since H and K are conjugate in $\mathrm{Hol}(A)$, by Lemma 17.4 there exists $\varphi \in \mathrm{Aut}(A)$ such that $\varphi H \varphi^{-1} = K$. The brace structure on A corresponding to the subgroup H is given by $a \circ b = a + f(b)$, where $(a, f) = (\pi_1|_H)^{-1}(a) \in H$, see Lemma **??**. Since

$$\varphi(f, a)\varphi^{-1} = (\varphi(a), \varphi \circ f \circ \varphi^{-1}) \in K,$$

it follows that $(\pi_1|_K)^{-1}(\varphi(a)) = (\varphi(a), \varphi \circ f \circ \varphi^{-1})$. Since $\varphi \in \mathrm{Aut}(A)$,

$$\begin{aligned}\varphi(a) \times \varphi(b) &= \varphi(a) + (\varphi \circ f \circ \varphi^{-1})(\varphi(b)) \\ &= \varphi(a) + \varphi(f(b)) = \varphi(a + f(b)) = \varphi(a \circ b)\end{aligned}$$

and hence the braces corresponding to H and K are isomorphic. $\square$

With Theorem 17.3, Lemma 17.4 and Proposition 17.5 one constructs small braces. In particular, the method can be used to compute the number $s(n)$ of non-isomorphic braces of size n. With small modifications, one computes the number $a(n)$ of non-isomorphic braces of abelian type of size n. Some values for $s(n)$ and $a(n)$ appear in Table 10.1.

§18. A universal construction

Table 10.1: The number of non-isomorphic braces.

n	1	2	3	4	5	6	7	8	9	10	11	12
$a(n)$	1	1	1	4	1	2	1	27	4	2	1	10
$s(n)$	1	1	1	4	1	6	1	47	4	6	1	38
n	13	14	15	16	17	18	19	20	21	22	23	24
$a(n)$	1	2	1	357	1	8	1	11	2	2	1	96
$s(n)$	1	6	1	1605	1	49	1	43	8	6	1	855
n	25	26	27	28	29	30	31	32	33	34	35	36
$a(n)$	4	2	37	9	1	4	1	25281	1	2	1	46
$s(n)$	4	6	101	29	1	36	1	1223061	1	6	1	400
n	37	38	39	40	41	42	43	44	45	46	47	48
$a(n)$	1	2	2	106	1	6	1	9	4	2	1	1708
$s(n)$	1	6	8	944	1	78	1	29	4	6	1	66209
n	49	50	51	52	53	54	55	56	57	58	59	60
$a(n)$	4	8	1	11	1	80	2	91	2	2	1	28
$s(n)$	4	51	1	43	1	1028	12	815	8	6	1	418
n	61	62	63	64	65	66	67	68	69	70	71	72
$a(n)$	1	2	11	?	1	4	1	11	1	4	1	489
$s(n)$	1	6	11	?	1	36	1	43	1	36	1	17790
n	73	74	75	76	77	78	79	80	81	82	83	84
$a(n)$	1	2	5	9	1	6	1	1985	804	2	1	34
$s(n)$	1	6	14	29	1	78	1	74120	8436	6	1	606
n	85	86	87	88	89	90	91	92	93	94	95	96
$a(n)$	1	2	1	90	1	16	1	9	2	2	1	195971
$s(n)$	1	6	1	800	1	294	1	29	8	6	1	?
n	97	98	99	100	101	102	103	104	105	106	107	108
$a(n)$	1	8	4	51	1	4	1	106	2	2	1	494
$s(n)$	1	53	4	711	1	36	1	944	8	6	1	11223
n	109	110	111	112	113	114	115	116	117	118	119	120
$a(n)$	1	6	2	1671	1	6	1	11	11	2	1	395
$s(n)$	1	94	8	65485	1	78	1	43	47	6	1	22711
n	121	122	123	124	125	126	127	128	129	130	131	132
$a(n)$	4	2	1	9	49	36	1	?	2	4	1	24
$s(n)$	4	6	1	29	213	990	1	?	8	36	1	324
n	133	134	135	136	137	138	139	140	141	142	143	144
$a(n)$	1	2	37	108	1	4	1	27	1	2	1	10215
$s(n)$	1	6	101	986	1	36	1	395	1	6	1	3013486
n	145	146	147	148	149	150	151	152	153	154	155	156
$a(n)$	1	2	9	11	1	19	1	90	4	4	2	40
$s(n)$	1	6	123	43	1	401	1	800	4	36	12	782
n	157	158	159	160	161	162	163	164	165	166	167	168
$a(n)$	1	2	1	209513	1	1374	1	11	2	2	1	443
$s(n)$	1	6	1	?	1	45472	1	43	12	6	1	28505

tab:braces

Some solutions

2.2 Let $G = \langle g \rangle$ be the cyclic group of order two. Then $1 - \frac{\sqrt{2}}{2} g$ is a non-trivial unit, as $\left(1 - \frac{\sqrt{2}}{2} g\right)\left(2 + \sqrt{2} g\right) = 1$.

10.5 Let $A = \{a\}$ and $B = \{b_1, \dots, b_m\}$. If AB admits a non-unique product, say $x = ab_i = ab_j$ with $i \neq j$, then $b_i = b_j$, a contradiction.

10.6 If AB admits a non-unique product $x = ab = a_1 b_1$, then so does $(gA)(Bh)$, as $(ga)(bh) = (ga_1)(b_1 h)$ is a non-unique product of $(gA)(Bh)$. The converse is trivial.

10.7 Assume that AB contains no unique products. By Exercise 10.6 we may assume that $A = \{1, a\}$ and $B = \{1, b_2, \dots, b_m\}$. We claim that $a^k \in B$ for all $k \geq 0$. We proceed by induction on k. The case $k = 0$ is easy, as $a^0 = 1 \in B$. Now if $a^k \in B$, then $a^{k+1} = aa^k \in AB$. Since G has no torsion and AB contains no unique products, $a^{k+1} = b_j$ for some j. It follows that $\{a^k : k \geq 0\} \subseteq B$, a contradiction.

14.9 The first claim follows from the compatibility condition (8.2) with $c = 1$. To prove the second claim let $d = b + c$. Then (8.2) becomes

$$a \circ d = a \circ b - a + a \circ (-b + d)$$

and the claim follows. The third claim is proved similarly.

14.10 The inverse of λ_a is given by $\lambda_a^{-1} \colon A \to A$, $b \mapsto a' \circ (a + b)$. To prove that $\lambda_a \in \operatorname{Aut}(A, +)$ we note that

$$\lambda_a(b + c) = -a + a \circ (b + c) = -a + a \circ b - a + a \circ c = \lambda_a(b) + \lambda_a(c).$$

Note that $\lambda_a(b) = -a + a \circ b = a \circ (a' + b)$, for all $a, b \in A$. Hence

$$\begin{aligned} \lambda_a(\lambda_b(c)) &= a \circ (a' + b \circ (b' + c)) = -a + a \circ b \circ (b' + c) \\ &= -a + a - a \circ b + a \circ b \circ c = -a \circ b + a \circ b \circ c = \lambda_{a \circ b}(c). \end{aligned}$$

14.11 Note that

$$\mu_a(b) = \lambda_b(a)' \circ b \circ a = (b \circ (b' + a))' \circ b \circ a = (b' + a)' \circ a,$$

for all $a, b \in A$. Hence μ_a is bijective and

$$\mu_a^{-1}(b) = ((b \circ a')' - a)' = (a \circ b' - a)' = (b' + a')' \circ a',$$

for all $a, b \in A$. Now we have

$$\begin{aligned} \mu_b(\mu_a(c)) &= \mu_b((c' + a)' \circ a) = (a' \circ (c' + a) + b)' \circ b \\ &= (a' \circ c' - a' + b)' \circ b = (a' \circ (c' + a \circ b))' \circ b \\ &= (c' + a \circ b)' \circ a \circ b = \mu_{a \circ b}(c), \end{aligned}$$

for all $a, b, c \in A$. Therefore the result follows.

15.13 Let $b \in A$ and $a \in \mathrm{Soc}(A)$. Since

$$b' \circ (b \circ a + b) = a - b' \text{ and } b' \circ (b + b \circ a) = -b' + a,$$

the first claim follows since $a \in Z(A, +)$. Now we prove the second claim:

$$b \circ a \circ b' = b \circ (a \circ b') = b \circ (a + b') = b \circ a - b = -b + b \circ a = \lambda_b(a).$$

17.2 We first prove that restriction restriction $\pi_1|_G$ of π_1 onto G is injective. Let $(a, f) \in G$ and $(b, g) \in G$ be such that $\pi_1(a, f) = \pi_1(b, g)$. Then $a = b$. Since G is a subgroup,

$$(-f^{-1}(a), f^{-1}) = (a, f)^{-1} \in G, \quad (-g^{-1}(a), g^{-1}) = (a, g)^{-1} \in G,$$

and hence $f = g$ since

$$(-f^{-1}(a), f^{-1}) \cdot a = 0 = (-g^{-1}(a), g^{-1}) \cdot a$$

and G is a regular subgroup. Now we prove that $\pi_1|_G$ is surjective. Let $a \in A$. Since G is regular, there exists $(x, f) \in G$ such that $x + f(a) = (x, f) \cdot a = 0$, so $(-f(a), f) \in G$ for some $f \in \mathrm{Aut}(A)$. Then $(a, f^{-1}) = (-f(a), f)^{-1} \in G$ and $\pi_2|_G(a, f^{-1}) = a$.

References

1. G. M. Bergman. Right orderable groups that are not locally indicable. *Pacific J. Math.*, 147(2):243–248, 1991.
2. S. J. Bigelow. Braid groups are linear. *J. Amer. Math. Soc.*, 14(2):471–486, 2001.
3. A. Clay and D. Rolfsen. *Ordered groups and topology*, volume 176 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2016.
4. The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.11.1*, 2021.
5. 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.
6. G. Gardam. A counterexample to the unit conjecture for group rings. *Ann. of Math. (2)*, 194(3):967–979, 2021.
7. 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.
8. M. Hertweck. A counterexample to the isomorphism problem for integral group rings. *Ann. of Math. (2)*, 154(1):115–138, 2001.
9. 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.
10. S. Kionke and J. Raimbault. On geometric aspects of diffuse groups. *Doc. Math.*, 21:873–915, 2016. With an appendix by Nathan Dunfield.
11. D. Krammer. Braid groups are linear. *Ann. of Math. (2)*, 155(1):131–156, 2002.
12. 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.
13. T. Y. Lam. *A first course in noncommutative rings*, volume 131 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1991.
14. D. S. Passman. *The algebraic structure of group rings*. Robert E. Krieger Publishing Co., Inc., Melbourne, FL, 1985. Reprint of the 1977 original.
15. 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