Leandro Vendramin

Groups, radical rings and the Yang–Baxter equation

A combinatorial approach to solutions

Wednesday 14th July, 2021

A Dino

The Yang–Baxter equation (YBE) arose from Yang's work on statistic mechanics. In 1967 Yang tried to find the eigenfunctions of a one-dimensional fermion gas with delta function inteaction. This was a rather difficult problem. He solved it and showed that a crucual identity in the intermediate steps was a matrix equation

$$A(u)B(u+v)A(v) = B(v)A(u+v)B(u).$$

Later, Baxter, in his solution of another problem in physics, the 8-vertex model again used the YBE. In 1980 Faddeev coined the term "Yang-Baxter Equation". A number of exciting developmenents in physics and mathematics have led to the conclusion that the YBE is a fundamental mathematical structure with connections to various subfields of mathematics such as knot theory, braid theory, operator theory, Hopf algebras, quantum groups, 3-manifolds, the monondromy of differential equations...

> I got the feeling that the YBE is the next pervasive algebraic equation after the Jacobi identity.

Compiled: Wednesday 14^{th} July, 2021, 21:24.

In Chapter 1 basic definitions and examples of solutions introduced. The main result of the chapter is Theorem 1.11, where the deep relationship between solutions and group actions is studied.

The first part of Chapter 2 provides an introduction to the theory of radical rings. The material presented is pretty standard. After recalling basic definitions and stating basic properties, the theory of the Jacobson radical is explored. The second part of the chapter is devoted to involutive solutions. One of the main results of this chapter is Rump's theorem, which states that radical rings produce solutions. In this chapter we also introduce cycle sets, which are structures that turns out to be equivalent to involutive solutions.

In Chapter 4 we introduce the theory of braces. One of the main results of this chapter is Theorem **??**, which proves that braces produce arbitrary solutions. We introduce skew cycle sets and prove in Theorem... that skew cycle sets and arbitrary solutions are equivalent.

In Chapter 5 we complements and 1-cocycles. In Theorem... Sysak's theorem states that...

The first part of Chapter 6 is devoted to the general theory of nilpotent groups. The second part is devoted to the Frattini subgroup and some of its applications The fourth part is about a sort of Frattini subgroup in the context of braces.

Chapter 7 is about solvable groups. The basic theory of solvable groups is presented in the first section. We prove Wielandt's three subgroups theorem and Hall's theorem.

Chapter **??** is about factorization of groups and braces. First we prove Itô's theorem in the case of groups: Every group that admits a factorization through two abelian subgroups is meta-abelian. The second section is about solvability of structure groups of involutive solutions and related concepts.

In Chapter 9 we prove one of the main results of the book. The existence of a universal brace that somewhat classifies solutions.

Thanks: Jingpeng Shen

Versión compilada el Wednesday 14th July, 2021 a las 21:24.

Leandro Vendramin
Buenos Aires, Argentina

Contents

Chapter 1
The Yang–Baxter equation

YB

A

In [29], Drinfeld briefly discuss set-theoretic solutions to the Yang–Baxter equation. He observed that it makes sense to consider the Yang–Baxter equation in the category of sets and that "maybe it would be interesting to study set-theoretical solutions".

Definition 1.1. A *set-theoretic solution* to the Yang–Baxter equation (YBE) is a pair (X,r), where X is a 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.

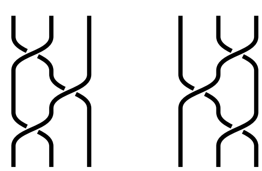


fig:braid

Figure 1.1: The Yang–Baxter equation.

For $n\geq 2$, the *braid group* $\mathbb{B}_n$ is defined as the group with generators $\sigma_1,\dots,\sigma_{n-1}$ and relations

$$\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} \qquad \text{if } 1 \leq i \leq n-2,$$
$$\sigma_i\sigma_j = \sigma_j\sigma_i \qquad \text{if } |i-j| \geq 1.$$

Let (X,r) be a set-theoretic solution to the YBE. Write $X^n = X \times \cdots \times X$ (n-times). For $i < n$ let $r_{i,i+1} = \mathrm{id}_{X^{i-1}} \times r \times \mathrm{id}_{X^{n-i-1}} \colon X^n \to X^n$. Then the map $\sigma_i \mapsto r_{i,i+1}$ extends to an action of $\mathbb{B}_n$ on X^n.

Example 1.2. Let X be a set. Then (X,r), where $r(x,y) = (y,x)$, is a 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 1.3.** *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*

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

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

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

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 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

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

Since (X,r^{-1}) is a solution, Lemma 1.3 implies that the following formulas hold:

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

Definition 1.4. 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. 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 1.5. We say that a 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 solution to the YBE.

lem:LYZ

Lemma 1.6. *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 $u = \sigma_x(y)$. $\square$

The bijectivity of r means that any row determines the whole square. Lemma 1.6 means that any column also determines the whole square, see Figure 1.2.

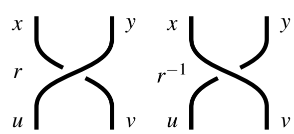


fig:braid

Figure 1.2: Any row or column determines the whole square.

Example 1.7. 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 1.8. 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:Wada

Example 1.9. Let G be a group. Then (G,r), where $r(x,y) = (xy^{-1}x^{-1}, xy^2)$, is a solution.

exa:Venkov

Example 1.10. Let G be a group. Then (G,r), where $r(x,y) = (xyx^{-1}, x)$, is a solution.

The now prove the main theorem of the chapter. The result shows an intriguing connection between group actions and non-degenerate solutions. It was proved by Lu, Yan and Zhu.

thm:LYZ **Theorem 1.11.** *Let G be a group and let $\xi\colon G\times G\to G$, $\xi(x,y)=x\triangleright y$, be a left action of G on itself, and let $\eta\colon G\times G\to G$, $\eta(x,y)=x\triangleleft y$, be a right action of G on itself. 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 bijective solution.

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 $v_1=v_2$. From Lemma 1.3 we note that

$$\begin{aligned} u_1&=(u\triangleright v)\triangleright((u\triangleleft v)\triangleright w), & v_1&=(u\triangleleft v)\triangleleft w,\\ u_2&=u\triangleright(v\triangleright w), & v_2&=(u\triangleleft(v\triangleright w))\triangleleft(v\triangleleft w). \end{aligned}$$

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,

$$v_2=u\triangleleft((v\triangleright w)(v\triangleleft w))=u\triangleleft(vw)=(u\triangleleft v)\triangleleft w=v_1.$$

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

Proposition 1.12. *Under the assumptions of Theorem 1.11, 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. In the proof of Theorem 1.11 we found that the inverse of r is given by $r^{-1} = \zeta \circ (i \times i) \circ r \circ (i \times i) \circ \zeta$, where $\zeta(x,y) = (y,x)$ and $i(x) = x^{-1}$, it follows that $r(x^{-1}, y^{-1}) = (u^{-1}, v^{-1})$. 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 follows that $yt = yv^{-1}$. Then $z = v^{-1}$. Similarly one proves $r(v, y^{-1}) = (u^{-1}, x)$. □

Exercises

prob:Wada **1.1.** Let G be a group. Prove that $r(x,y) = (xy^{-1}x^{-1}, xy^2)$ is involutive if and only if $x^2 = 1$ for all $x \in G$.

1.2. Let X be a finite non-empty set and $r\colon X \times X \to X \times X$, $(x,y) \mapsto (\sigma_x(y), \tau_y(x))$, be a map. Prove that (X,r) is a solution if and only if the maps $\sigma_x\colon X \to X$ are bijective for all $x \in X$, $r^2 = \mathrm{id}_{X \times X}$ and

$$\sigma_x \circ \sigma_{\sigma_x^{-1}(y)} = \sigma_y \circ \sigma_{\sigma_y^{-1}(x)}$$

for all $x, y \in X$.

1.3. Prove that if (X,r) be a solution...? FIXME

prob:perm_group **1.4.** Let (X,r) be a solution. Prove that $\mathscr{G}(X,r) \simeq \langle (\sigma_x, \tau_x^{-1}) : x \in X \rangle$.

Notes

The first papers where set-theoretic solutions are studied are those of Etingof, Schedler and Soloviev [32] and Gateva–Ivanova and Van den Bergh [36]. Both papers deal with non-degenerate involutive solutions.

In [29], Drinfeld attributes Example 1.8 to Lyubashenko. Example 1.9 appears in the work of Wada [68]. Proposition 2.55 was proved by Rump [56].

Theorem 1.11 goes back to Lu, Yan and Zhu, see [48]. Similar results can be found in the work of Etingof, Schedler and Soloviev [32] for involutive solutions and in Soloviev's paper [64].

Chapter 2
Radical rings

radical

A

We will consider rings possibly without identity. Thus a **ring** is an abelian group R with an associative multiplication $(x,y) \mapsto xy$ such that $(x+y)z = xz+yz$ and $x(y+z) = xy+xz$ for all $x,y,z \in R$. If there is an element $1 \in R$ such that $x1 = 1x = x$ for all $x \in R$, we say that R is a ring (or a unitary ring). A **subring** S of R is an additive subgroup of R closed under multiplication.

Example 2.1. $2\mathbb{Z} = \{2m : m \in \mathbb{Z}\}$ is a ring.

A **left ideal** (resp. **right ideal**) is a subring I of R such that $rI \subseteq I$ (resp. $Ir \subseteq I$) for all $r \in R$. An **ideal** (also two-sided ideal) of R is a subring I of R that is both a left and a right ideal of R.

Example 2.2. If I and J are both ideals of R, then the sum $I+J = \{x+y : x \in I, y \in J\}$ and the intersection $I \cap J$ are both ideals of R. The product IJ, defined as the additive subgroup of R generated by $\{xy : x \in I, y \in J\}$, is also an ideal of R.

Example 2.3. If R is a ring, the set $Ra = \{xa : x \in R\}$ is a left ideal of R. Similarly, the set $aR = \{ax : x \in R\}$ is a right ideal of R. The set RaR, which is defined as the additive subgroup of R generated by $\{xay : x,y \in R\}$, is a ideal of R.

Example 2.4. Ir R is a unitary ring, then Ra is the left ideal generated by a, aR is the right ideal generated by a and RaR is the ideal generated by a. If R is not unitary, the left ideal generated by a is $Ra + \mathbb{Z}a$, the right ideal generated by a is $aR + \mathbb{Z}a$ and the ideal generated by a is $RaR + Ra + aR + \mathbb{Z}a$.

A ring R is said to be **simple** if $R^2 \neq \{0\}$ and the only ideals of R are 0 and R. The condition $R^2 \neq \{0\}$ is trivially satisfied in the case of rings with identity, as $1 \in R^2$.

Example 2.5. Division rings are simple.

Let S be a unitary ring. Recall that $M_n(S)$ is the ring of $n\times n$ square matrices with entries in S. If $A=(a_{ij})\in M_n(S)$ y E_{ij} is the matrix such that $(E_{ij})_{kl}=\delta_{ik}\delta_{jl}$, then

$$E_{ij}AE_{kl}=a_{jk}E_{il} \tag{2.1}$$ eq:trick

for all $i,j,k,l\in\{1,\dots,n\}$.

Exercise 2.6. If D is a division ring, then $M_n(D)$ is simple.

Let R be a ring. A left R-module (or module, for short) is an abelian group M together with a map $R\times M\to M$, $(r,m)\mapsto rm$, such that

$$(r+s)m=rm+sm,\qquad r(m+n)=rm+rs,\qquad r(sm)=(rs)m$$

for all $r,s\in R$, $m,n\in M$. If R has an identity 1 and $1m=m$ holds for all $m\in M$, the module M is said to be **unitary**. If M is a unitary module, then $M=RM\neq\{0\}$.

The module M is said to be **simple** if $RM\neq\{0\}$ and the only submodules of M are 0 and M. If M is a simple module, then $M\neq\{0\}$.

lemma:simple **Lemma 2.7.** *Let M be a non-zero module. Then M is simple if and only if $M=Rm$ for all $0\neq m\in M$.*

Proof. Assume that M is simple. Let $m\neq 0$. Since Rm is a submodule of the simple module M, either $Rm=0$ or $Rm=M$. Let $N=\{n\in M:Rn=0\}$. Since N is a submodule of M and $RM\neq\{0\}$, $N=\{0\}$. Therefore $Rm=M$s, as $m\neq 0$. Now assume that $M=Rm$ for all $m\neq 0$. Let L be a non-zero submodule of M and let $0\neq x\in L$. Then $M=L$, as $M=Rx\subseteq L$. □

Example 2.8. Let D be a division ring and let V be a non-zero vector space (over D). If $R=\mathrm{End}_D(V)$, then V is a simple R-módulo with $fv=f(v)$, $f\in R$. $v\in V$.

exa:I_k **Example 2.9.** Let $n\geq 2$. If D is a division ring and $R=M_n(D)$, then each

$$I_k=\{(a_{ij})\in R:a_{ij}=0 \text{ para } j\neq k\}$$

is an R-module isomorphic to D^n. Thus $M_n(D)$ is a simple ring that is not a simple $M_n(D)$-module.

A left ideal L of a ring R is said to be **minimal** if $L\neq\{0\}$ and L does not strictly contain other left ideals of R. Similarly one defines right minimal ideals and minimal ideals.

Example 2.10. Let D be a division ring and let $R=M_n(D)$. Then $L=RE_{11}$ is a minimal left ideal.

Example 2.11. Let L be a non-zero left ideal. If $RL\neq\{0\}$, then L is minimal if and only if L is a simple R-module.

A left (resp. right) ideal L of R is said to be **regular** if there exists $e \in R$ such that $r - re \in L$ (resp. $r - er \in L$) for all $r \in R$. If R is a ring with identity, every left (or right) ideal is regular. A left (resp. right) ideal I of R is said to be **maximal** if $I \neq M$ and I is not properly contained in any other left (resp. right) ideal of R. A standard application of Zorn's lemma proves that every unitary ring contains a maximal left (or right) ideal. Similarly one defines maximal ideals.

proposition:R/I

Proposition 2.12. *Let R be a ring and M be a module. Then M is simple if and only if $M \simeq R/I$ for some maximal regular left ideal I.*

Proof. Assume that M is simple. Then $M = Rm$ for some $m \neq 0$ by Lemma 2.7. The map $\phi\colon R \to M$, $r \mapsto rm$, is an epimorphism of R-modules, so the first isomorphism theorem implies that $M \simeq R/\ker\phi$.

We claim that $I = \ker\phi$ is a maximal ideal. The correspondence theorem and the simpllicity of M imply that I is a maximal ideal (because each left ideal J such that $I \subseteq J$ yields a submodule of R/I).

We claim that I is regular. Since $M = Rm$, there exists $e \in R$ such that $m = em$. If $r \in R$, then $r - re \in I$ since $\phi(r - re) = \phi(r) - \phi(re) = rm - r(em) = 0$.

Supongamos ahora que L es maximal y regular. Por el teorema de la correspondencia, R/L no tiene submódulos propios no nulos. Veamos entonces que $R(R/L) \neq 0$. Si $R(R/L) = 0$ y $r \in R$, entonces, como L es regular, $r - re \in L$ y luego $r \in L$ pues

$$0 = r(e+I) = re + I = r + I,$$

una contradicción a la maximalidad de L. $\square$

We will now discuss primitive rings.

Let R be a ring and M be a left R-module. For a subset $N \subseteq M$ we define the **annihilator** of N as the subset

$$\mathrm{Ann}_R(N) = \{r \in R : rn = 0\ \forall n \in N\}.$$

Example 2.13. $\mathrm{Ann}_{\mathbb{Z}}(\mathbb{Z}/n) = n\mathbb{Z}$.

The following exercise is standard.

Exercise 2.14. Let R be a ring and M be a module. If $N \subseteq M$ is a subset, then $\mathrm{Ann}_R(N)$ is a left ideal of R. If $N \subseteq M$ is a submodule of R, then $\mathrm{Ann}_R(N)$ is an ideal of R.

A module M is said to be **faithful** if $\mathrm{Ann}_R(M) = \{0\}$.

Example 2.15. If K is a field, then K^n is a faithful unitary $M_n(K)$-module.

Example 2.16. If V is vector space over a field K, then V is faithful unitary $\mathrm{End}_K(V)$-module.

A ring R is said to be **primitive** if there exists a faithful simple R-módulo. Since we are considering left modules, our definition of primitive rings is that of left primitive rings. By convention, a primitive ring will always mean a left primitive ring. The use of right modules yields to the notion of right primitive rings.

proposition:simple=>prim

Proposition 2.17. *If R is a simple unitary ring, then R is primitive.*

Proof. Since R is unitary, there exists a maximal left ideal I and, moreover, R is regular. By Proposition 2.12, R/I is a simple R-module. Since $\mathrm{Ann}_R(R/I)$ is an ideal of R and R is simple, either $\mathrm{Ann}_R(R/I) \in \{0\}$ or $\mathrm{Ann}_R(R/I) = R$. Moreover, since $1 \notin \mathrm{Ann}(R/I)$, it follows that $\mathrm{Ann}_R(R/I) = \{0\}$. □

osition:prim+conm=cuerpo

Proposition 2.18. *If R is a commutative ring, then R is primitive if and only if R is a field.*

Proof. If R is a field, then R is primitive because it is a unitary simple ring, see Proposition 2.17. If R is a primitive commutative ring, Proposition 2.12 implies that there exists a maximal regular ideal I such that R/I is a faithful simple R-module. Since $I \subseteq \mathrm{Ann}_R(R/I) = \{0\}$ and I is regular, there exists $e \in R$ such that $r = re = er$. Therefore R is a unitary commutative ring. Since $I = \{0\}$ is a maximal ideal, R is a field. □

Example 2.19. The ring $\mathbb{Z}$ is not primitive.

An ideal P of a ring R is said to be **primitive** if $P = \mathrm{Ann}_R(M)$ for some simple R-module M.

lemma:primitivo

Lemma 2.20. *Let R be a ring and P be an ideal of R. Then P is primitive if and only if R/P is a primitive ring.*

Proof. Assume that $P = \mathrm{Ann}_R(M)$ for some R-module M. Then M is a simple R/P-module with $(r+P)m = rm$, $r \in R$, $m \in M$. This is well-defined, as $P = \mathrm{Ann}_R(M)$. Since M is a simple R-module, it follows that M is a simple R/P-module. Moreover, $\mathrm{Ann}_{R/P} M = \{0\}$. Indeed, if $(r+P)M = 0$, then $r \in \mathrm{Ann}_R M = P$ and hence $r+P = P$.

Assume now that R/P is primitive. Let M be a faithful simple R/P-module. Then $rm = (r+P)m$, $r \in R$, $m \in M$, turns M into an R-module. It follows that M is simple and that $P = \mathrm{Ann}_R(M)$. □

Example 2.21. Let $R_1, \dots, R_n$ be primitive ring and $R = R_1 \times \cdots \times R_n$. Then each $P_i = R_1 \times \cdots \times R_{i-1} \times \{0\} \times R_{i+1} \times \cdots \times R_n$ is a primitive ideal of R since $R/P_i \simeq R_i$.

lemma:maxprim

Lemma 2.22. *Let R be a ring. Si P es un ideal primitivo, existe un ideal a izquierda L maximal tal que $P = \{x \in R : xR \subseteq L\}$. Recíprocamente, si L es un ideal a izquierda maximal y regular, entonces $\{x \in R : xR \subseteq L\}$ es un ideal primitivo.*

Proof. Assume that $P = \mathrm{Ann}_R(M)$ for some simple R-module M. By Proposition 2.12, there exists a regular maximal left ideal L such that $M \simeq R/L$. Then $P = \mathrm{Ann}_R(R/L) = \{x \in R : xR \subseteq L\}$.

Conversely, let L a regular maximal left ideal.By Proposition 2.12, R/L is a simple R-module simple. Then

$$\mathrm{Ann}_R(R/L) = \{x \in R : xR \subseteq L\}$$

if a primitive ideal. □

Proposition 2.23. *Maximal ideals of unitary rings are primitive.*

Proof. Let R be a ring with identity and M be a maximal ideal of R. Then R/M is a simple unitary ring by Proposition 2.12. Then R/M is primitive by Proposition 2.17. By lema 2.20, M is primitive. □

Exercise 2.24. Prove that every primitive ideal of a commutative ring is maximal.

Exercise 2.25. Prove that $M_n(R)$ is primitive if and only if R is primitive.

Let us discuss the Jacobson radical and radical rings.

Let R be a ring. The **Jacobson radical** $J(R)$ is the intersection of all the annihilators of simple left R-modules. If R does not have simple left R-modules, then $J(R) = R$. From the definition it follows that $J(R)$ is an ideal. Moreover,

$$J(R) = \bigcap \{P : P \text{ left primitive ideal}\}.$$

If I is an ideal of R and $n \in \mathbb{N}$, I^n is the additive subgroup of R generated by the set $\{y_1 \dots y_n : y_j \in I\}$. An ideal I of R is **nilpotent** if $I^n = \{0\}$ for some $n \in \mathbb{N}$. Similarly one defines right or left nil ideals. Note that an ideal I is nilpotent if and only if there exists $n \in \mathbb{N}$ such that $x_1 x_2 \cdots x_n = 0$ for all $x_1, \dots, x_n \in I$.

An element x of a ring is said to be **nil** (or nilpotent) if $x^n = 0$ for some $n \in \mathbb{N}$. An ideal I of a ring is said to be nil if every element of I is nil. Every nilpotent ideal is nil, as $I^n = 0$ implies $x^n = 0$ for all $x \in I$.

Example 2.26. Let $R = \mathbb{C}[x_1, x_2, \dots]/(x_1, x_2^2, x_3^3, \dots)$. The ideal $I = (x_1, x_2, x_3, \dots)$ is nil in R, as it is generated by nilpotent element. However, it is not nilpotente. Indeed, if I is nilpotent, then there exists $k \in \mathbb{N}$ such that $I^k = 0$ and hence $x_i^k = 0$ for all i, a contradiction since $x_{k+1}^k \neq 0$.

pro:nilJ **Proposition 2.27.** *Let R be a ring. Then every nil left ideal (resp. right ideal) is contained in $J(R)$.*

Proof. Assume that there is a nil left ideal (resp. right ideal) I such that $I \not\subseteq J(R)$. There exists a simple R-module M such that $n = xm \neq 0$ for some $x \in I$ and some $m \in M$. Since M is simple, $Rn = M$ and hence there exists $r \in R$ such that

$$(rx)m = r(xm) = rn = m \quad (\text{resp. } (xr)n = x(rn) = xm = n).$$

Thus $(rx)^k m = m$ (resp. $(xr)^k n = n$) for all $k \geq 1$, a contradiction since $rx \in I$ (resp. $xr \in I$) is a nilpotent element. □

Let R be a ring. An element $a \in R$ is said to be **left quasi-regular** if there exists $r \in R$ such that $r + a + ra = 0$. Similarly, a is said to be **right quasi-regular** if there exists $r \in R$ such that $a + r + ar = 0$.

exercise:circc

Exercise 2.28. Let R be a ring. Prove that $R \times R \to R$, $(r,s) \mapsto r \circ s = r + s + rs$, is an associative operation with neutral element 0.

Exercise 2.29. Let $R = \mathbb{Z}/3 = \{0,1,2\}$. Compute the multiplication table with respect to the circle operation given by the previous exercise.

If R is unitary, an element $x \in R$ is left quasi-regular (resp. right quasi-regular) if and only if $1 + x$ is left invertible (resp. right invertible). In fact, if $r \in R$ is such that $r + x + rx = 0$, then $(1 + r)(1 + x) = 1 + r + x + rx = 1$. Conversely, if there exists $y \in R$ such that $y(1 + x) = 1$, then

$$(y-1) \circ x = y - 1 + x + (y-1)x = 0.$$

Example 2.30. If $x \in R$ is a nilpotent element, then $y = \sum_{n \geq 1} x^n \in R$ is quasi-regular. En efecto, si existe N tal que $x^N = 0$, la suma que define al elemento y es finita y cumple que $y + (-x) + y(-x) = 0$.

A left ideal I of R is said to be **left quasi-regular** (resp. right quasi-regular) if every element of I is left quasi-regular (resp. right quasi-regular). A left ideal is said to be **quasi-regular** if it is left and right quasi-regular. Similarly one defines right quasi-regular ideals and quasi-regular ideals.

lemma:casiregular

Lemma 2.31. *Let I be a left ideal of R. If I is left quasi-regular, then I is quasi-regular.*

Proof. Let $x \in I$. Let us prove that x is right quasi-regular. Since I is left quasi-regular, there exists $r \in R$ such that $r \circ x = r + x + rx = 0$. Since $r = -x - rx \in I$, there exists $s \in R$ tal que $s \circ r = s + r + sr = 0$. Then s is right quasi-regular and

$$x = 0 \circ x = (s \circ r) \circ x = s \circ (r \circ x) = s \circ 0 = s. \qquad \square$$

Let $(A, \leq)$ be a partially order set, this means that A is a set together with a reflexive, transitive and anti-symmetric binary relation R en $A \times A$, where $a \leq b$ if and only if $(a,b) \in R$. Recall that the relation is reflexive if $a \leq a$ for all $a \in A$, the relation is transitive if $a \leq b$ and $b \leq c$ imply that $a \leq c$ and the relation is anti-symmetric if $a \leq b$ and $b \leq a$ imply $a = b$.

The elements $a, b \in A$ are said to be **comparable** if $a \leq b$ or $b \leq a$. An element $a \in A$ is said to be **maximal** if $c \leq a$ for all $c \in A$ that is comparable with a. An **upper bound** for a non-empty subset $B \subseteq A$ is an element $d \in A$ such that $b \leq d$ for all $b \in B$. A **chain** in A is a subset B such that every pair of elements of B are comparable. **Zorn's lemma** states the following property:

> If A is a non-empty partially ordered set such that every chain in A contains an upper bound in A, then A contains a maximal element.

Our application of Zorn's lemma:

lemma:maxreg

Lemma 2.32. *Let R be a ring and $x \in R$ be an element that is not left quasi-regular Then there exists a maximal left ideal M such that $x \notin M$. Moreover, R/M is a simple R-module and $x \notin \operatorname{Ann}_R(R/M)$.*

Proof. Let $T = \{r + rx : r \in R\}$. A straightforward calculation shows that T is a left ideal of R such that $x \notin T$ (if $x \in T$, then $r + rx = -x$ for some $r \in R$, a contradiction since x is not left quasi-regular).

The only left ideal of R contanining $T \cup \{x\}$ is R. Indeed, if there exists a left ideal U containing T, then $x \notin U$, since otherwise every $r \in R$ could be written as $r = (r + rx) + r(-x) \in U$.

Let $\mathscr{S}$ be the set of proper left ideals of R containing T partially ordered by inclusion. If $\{K_i : i \in I\}$ is a chain in $\mathscr{S}$, then $K = \cup_{i \in I} K_i$ is an upper bound for the chain (K is a proper, as $x \notin K$). Zorn's lemma implies that $\mathscr{S}$ admits a maximal element M. Thus M is a maximal left ideal such that $x \notin M$. Moreover, M is regular since $r + r(-x) \in T \subseteq M$ for all $r \in R$. Therefore R/M is a simple R-module by Proposition 2.12. Since $x(x+M) \neq 0$ (if $x^2 \in M$, then $x \in M$, as $x + x^2 \in T \subseteq M$), it follows that $x \notin \operatorname{Ann}_R(R/M)$. □

If $x \in R$ is not left quasi-regular, Lemma 2.32 implies that there exists a simple R-module M such $x \notin \operatorname{Ann}_R(M)$. Thus $x \notin J(R)$.

thm:casireg_eq

Theorem 2.33. *Let R be a ring and $x \in R$. The following statements are equivalent:*

1) *The left ideal generated by x is quasi-regular.*
2) *Rx is quasi-regular.*
3) *$x \in J(R)$.*

Proof. The implication $(1) \implies (2)$ is trivial, as Rx is included in the left ideal generated by x.

We now prove $(2) \implies (3)$. If $x \notin J(R)$, then Lemma 2.32 implies that there exists a simple R-module M such that $xm \neq 0$ for some $m \in M$. The simplicity of M implies that $R(xm) = M$. Thus there exists $r \in R$ such that $rxm = -m$. There is an element $s \in R$ such that $s + rx + s(rx) = 0$ and hence

$$-m = rxm = (-s - srx)m = -sm + sm = 0,$$

a contradiction.

Finally, to prove $(3) \implies (1)$ it is enough to note that x is left quasi-regular. Thus the left ideal generated by x is quasi-regular by Lemma 2.31. □

The theorem immediately implies the following corollary.

Corollary 2.34. *If R is a ring, then $J(R)$ if a quasi-regular ideal that contains every left quasi-regular ideal.*

The following result is somewhat what we all had in mind.

thm:J(R)

Theorem 2.35. *Let R be a ring such that $J(R) \neq R$. Then*

$$J(R) = \bigcap \{I : I \text{ regular maximal left ideal of } R\}.$$

Proof. We only prove the non-trivial inclusion. Let

$$K = \bigcap \{I : I \text{ regular maximal left ideal of } R\}.$$

By Proposition 2.12,

$$J(R) = \bigcap \{\mathrm{Ann}_R(R/I) : I \text{ regular maximal left ideal of } R\}.$$

Let I be a regular maximal left ideal. If $r \in J(R) \subseteq \mathrm{Ann}_R(R/I)$, then, since I is regular, there exists $e \in R$ such that $r - re \in I$. Since

$$re + I = r(e+I) = 0,$$

$re \in I$ and hence $r \in I$. Thus $J(R) \subseteq K$. $\square$

Example 2.36. Each maximal ideals of $\mathbb{Z}$ is of the form $p\mathbb{Z} = \{pm : m \in \mathbb{Z}\}$ for some prime number p. Thus $J(\mathbb{Z}) = \cap_p p\mathbb{Z} = \{0\}$.

We now review some basic results useful to compute radicals.

Proposition 2.37. *Let $\{R_i : i \in I\}$ be a family of rings. Then*

$$J\left(\prod_{i \in I} R_i\right) = \prod_{i \in I} J(R_i).$$

Proof. Let $R = \prod_{i \in I} R_i$ and $x = (x_i)_{i \in I} \in R$. The left ideal Rx is quasi-regular if and only if each left ideal $R_i x_i$ is quasi-regular in R_i, as x is quasi-regular in R if and only if each x_i is quasi-regular in R_i. Thus $x \in J(R)$ if and only if $x_i \in J(R_i)$ for all $i \in I$. $\square$

For the next result we shall need a lemma.

lemma:trickJ1

Lemma 2.38. *Let R be a ring and $x \in R$. If $-x^2$ is a left quasi-regular element, then x también.*

Proof. Sea $r \in R$ tal que $r + (-x^2) + r(-x^2) = 0$ y sea $s = r - x - rx$. Entonces x es casi-regular a izquierda pues

$$\begin{aligned} s + x + sx &= (r - x - rx) + x + (r - x - rx)x \\ &= r - x - rx + x + rx - x^2 - rx^2 = r - x^2 - rx^2 = 0. \end{aligned}$$ $\square$

proposition:J(I)

Proposition 2.39. *If I is an ideal of R, then $J(I) = I \cap J(R)$.*

Proof. Since $I \cap J(R)$ if an ideal of I, if $x \in I \cap J(R)$, then x is left quasi-regular in R. Let $r \in R$ be such that $r + x + rx = 0$. Since $r = -x - rx \in I$, x is left quasi-regular in I. Thus $I \cap J(R) \subseteq J(I)$.

Let $x \in J(I)$ and $r \in R$. Since $-(rx)^2 = (-rxr)x \in I(J(I)) \subseteq J(I)$, the element $-(rx)^2$ is left quasi-regular a izquierda en I. Thus rx is left quasi-regular by Lemma 2.38. $\square$

A ring R is said to be **radical** if $J(R) = R$.

Example 2.40. If R is a ring, then $J(R)$ is a radical ring, by Proposition 2.39.

Example 2.41. The Jacobson radical of $\mathbb{Z}/8$ is $\{0,2,4,6\}$.

There are several characterizations of radical rings.

theorem:anillo_radical

Theorem 2.42. *Let R be ring. The following statements are equivalent:*

1) *R is radical.*
2) *R admits no simple R-modules.*
3) *R no tiene ideales a izquierda maximales y regulares.*
4) *R no tiene ideales a izquierda primitivos.*
5) *Every element of R is quasi-regular.*
6) *$(R, \circ)$ is a group.*

Proof. The equivalence $(1) \iff (5)$ follows from Theorem 2.33.

The equivalence $(5) \iff (6)$ is left as an exercise.

Let us prove that $(1) \implies (2)$. Assume that there exists a simple R-module N. Since $R = J(R) \subseteq \mathrm{Ann}_R(N)$, $R = \mathrm{Ann}_S(N)$. Hence $RN = \{0\}$, a contradiction to the simplicity of N.

To prove $(2) \implies (3)$ we note that for each regular and maximal left ideal I, the quotient R/I is a simple R-module by Proposición 2.12.

To prove $(3) \implies (4)$ assume that there is a primitive left ideal $I = \mathrm{Ann}_R(M)$, where M is some simple R-module. Since $R = J(R) \subseteq I$, it follows that $I = R$, a contradiction to the simplicity of M.

Finally we prove $(4) \implies (2)$. If M is a simple R-module, then $\mathrm{Ann}_R(M)$ is a primitive left ideal. $\square$

Example 2.43. Let

$$A = \left\{ \frac{2x}{2y+1} : x, y \in \mathbb{Z} \right\}.$$

Then A is a radical ring, as the inverse of the element $\frac{2x}{2y+1}$ with respect to the circle operation $\circ$ is

$$\left(\frac{2x}{2y+1} \right)' = \frac{-2x}{2(x+y)+1}.$$

A ring R is said to be **nil** if for every $x \in R$ there exists $n = n(x)$ such that $x^n = 0$.

Exercise 2.44. Prove that a nil ring is a radical ring.

Exercise 2.45. Let $\mathbb{R}[X]$ be the ring of power series with real coefficients. Prove that the ideal $X\mathbb{R}[X]$ consisting of power series with zero constant term is a radical ring that is not nil.

The following problem is maybe the most important open problem in non-commutative ring theory.

The conjecture is known to be true in several cases. $\boxed{\text{Exercises?}}$

thm:Jnilpotente

Theorem 2.46. *If R is a left artinian ring, then $J(R)$ is nilpotent.*

Proof. Let $J = J(R)$. Since R is a left artinian ring, the sequence $(J^m)_{m\in\mathbb{N}}$ of left ideals stabilizes. There exists $k \in \mathbb{N}$ such that $J^k = J^l$ for all $l \geq k$. We claim that $J^k = \{0\}$. If $J^k \neq \{0\}$ let $\mathscr{S}$ the set of left ideals I such that $J^k I \neq \{0\}$. Since

$$J^k J^k = J^{2k} = J^k \neq \{0\},$$

the set $\mathscr{S}$ is non-empty. Since R is left artinian, $\mathscr{S}$ has a minimal element I_0. Since $J^k I_0 \neq \{0\}$, let $x \in I_0 \setminus \{0\}$ be such that $J^k x \neq \{0\}$. Moreover, $J^k x$ is a left ideal of R contained in I_0 and such that $J^k x \in \mathscr{S}$, as $J^k(J^k x) = J^{2k}x = J^k x \neq \{0\}$. The minimality of I_0 implies that, $J^k x = I_0$. In particular, there exists $r \in J^k \subseteq J(R)$ such that $rx = x$. Since $-r \in J(R)$ is left quasi-regular, there exists $s \in R$ such that $s - r - sr = 0$. Thus

$$x = rx = (s - sr)x = sx - s(rx) = sx - sx = 0,$$

a contradiction. □

Corollary 2.47. *Let R be a left artinian ring. Each nil left ideal is nilpotent and $J(R)$ is the unique maximal nilpotent ideal of R.*

Proof. Let L be a nil left ideal of R. By Proposition 2.27, L is contained in $J(R)$. Thus L is nilpotent, as $J(R)$ is nilpotent by Theorem 2.46. □

Theorem 2.48. *Let R be a ring and $n \in \mathbb{N}$. Then $J(M_n(R)) = M_n(J(R))$.*

Proof. We first prove that $J(M_n(R)) \subseteq M_n(J(R))$. If $J(R) = R$, the theorem is clear. Let us assume that $J(R) \neq R$ and let $J = J(R)$. If M is a simple R-module, then M^n is a simple $M_n(R)$-module with the usual multiplication. Let $x = (x_{ij}) \in J(M_n(R))$ and $m_1, \dots, m_n \in M$. Then

$$x \begin{pmatrix} m_1 \\ \vdots \\ m_n \end{pmatrix} = 0.$$

In particular, $x_{ij} \in \operatorname{Ann}_R(M)$ for all $i, j \in \{1, \dots, n\}$. Hence $x \in M_n(J)$.

We now prove that $M_n(J) \subseteq J(M_n(R))$. Let

$$J_1 = \begin{pmatrix} J & 0 & \cdots & 0 \\ J & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ J & 0 & \cdots & 0 \end{pmatrix} \quad \text{and} \quad x = \begin{pmatrix} x_1 & 0 & \cdots & 0 \\ x_2 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ x_n & 0 & \cdots & 0 \end{pmatrix} \in J_1.$$

Since x_1 es quasi-regular, there exists $y_1 \in R$ such that $x_1 + y_1 + x_1 y_1 = 0$. If

$$y = \begin{pmatrix} y_1 & 0 & \cdots & 0 \\ 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 \end{pmatrix},$$

then $u = x + y + xy$ is lower triangular, as

$$u = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ x_2 y_1 & 0 & \cdots & 0 \\ x_3 y_1 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ x_n y_1 & 0 & \cdots & 0 \end{pmatrix}.$$

Since $u^n = 0$, the element

$$v = -u + u^2 - u^3 + \cdots + (-1)^{n-1} u^{n-1}$$

is such that $u + v + uv = 0$. Thus x is right quasi-regular, as

$$x + (y + v + yv) + x(y + v + yv) = 0,$$

and therefore J_1 is right quasi-regular. Similarly one proves that each J_i is right quasi-regular and hence $J_i \subseteq J(M_n(R))$ for all $i \in \{1, \ldots, n\}$. In conclusion,

$$J_1 + \cdots + J_n \subseteq J(M_n(R))$$

and therefore $M_n(J) \subseteq J(M_n(R))$. $\square$

For completeness we recall basic results on the Jacobson radical in the case of unitary rings.

Exercise 2.49. Let R be a unitary ring. Then

$$J(R) = \bigcap \{M : M \text{ is a left maximal ideal}\}.$$

Exercise 2.50. Let R be a unitary ring. The following statements are equivalent:

1) $x \in J(R)$.
2) $xM = 0$ for all simple R-module M.
3) $x \in P$ for all primitive left ideal P.
4) $1 + rx$ is invertible for all $r \in R$.
5) $1 + \sum_{i=1}^{n} r_i x s_i$ is invertible for all $n \in \mathbb{N}$ and all $r_i, s_i \in R$.
6) x belongs to every left maximal ideal maximal.

B

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

Definition 2.51. A solution (X,r) is said to be *involutive* if $r^2 = \mathrm{id}$.

For $n \geq 2$, the *symmetric group* $\mathbb{S}_n$ can be presented as the group with generators $\sigma_1, \dots, \sigma_{n-1}$ and relations

$$\begin{aligned} &\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1} && \text{if } 1 \leq i \leq n-2,\\ &\sigma_i\sigma_j = \sigma_j\sigma_i && \text{if } |i-j| \geq 1,\\ &\sigma_i^2 = 1 && \text{for all } i \in \{1,\dots,n-1\}. \end{aligned}$$

Let (X,r) be an involutive solution. Then the map $\sigma_i \mapsto r_{i,i+1} = \mathrm{id}_{X^{i-1}} \times r \times \mathrm{id}_{X^{n-i-1}}$ extends to an action of $\mathbb{S}_n$ on X^n.

Example 2.52. 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. These examples show an intriguing connection between the YBE and the theory of non-commutative rings.

Example 2.53. Let p be a prime and let $A = \mathbb{Z}/(p^2)$ be the cylic additive group of order p^2. The operation $x \circ y = x + y + pxy$ turns A into a radical ring.

Example 2.54. Let $A = \left\{ \frac{2x}{2y+1} : x,y \in \mathbb{Z} \right\}$. The operation $a \circ b = a + b + ab$ turns A into a radical ring. A straightforward computation shows that

$$\left(\frac{x}{2y+1}\right)' = \frac{2(-x)}{2(x+y)+1}.$$

The following fundamental family of solutions appears in [56]. It turns out to be fundamental in the study of set-theoretic solutions to the YBE.

pro:Rump **Proposition 2.55.** *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 1.11, see Exercise 2.2. We will prove a stronger result in Theorem 4.22.

pro:T **Proposition 2.56.** *Let (X,r) be an involutive solution. Then the map $T \colon X \to X$, $x \mapsto \sigma_x^{-1}(x)$, is invertible with inverse $T^{-1}(y) = \tau_y^{-1}(y)$ and*

$$T^{-1} \circ \sigma_x^{-1} \circ T = \tau_x$$

for all $x \in X$*.*

Proof. Let $U(x) = \tau_x^{-1}(x)$. Since r is involutive,

$$(U(x), x) = r^2(U(x), x) = r(\sigma_{U(x)}(x), x) = (\sigma_{\sigma_{U(x)}(x)}(x), \tau_x \sigma_{U(x)}(x)).$$

The second coordinate can be written as $U(x) = \sigma_{U(x)}(x)$. This implies that

$$T(U(x)) = \sigma_{U(x)}^{-1}(U(x)) = x.$$

Similarly one obtains $U(T(x)) = x$.

Since (X, r) is a solution, Lemma 1.3 implies that $\sigma_x \sigma_y = \sigma_{\sigma_x(y)} \sigma_{\tau_y(x)}$ holds for all $x, y \in X$. Then

$$\sigma_y^{-1} T(x) = \sigma_y^{-1} \sigma_x^{-1}(x) = \sigma_{\tau_y(x)}^{-1} \sigma_{\sigma_x(y)}^{-1}(x) = \sigma_{\tau_y(x)}^{-1} \tau_y(x) = T \tau_y(x)$$

for all $y \in X$, by Equality (2.2). □

Note that if (X, r) is a non-degenerate 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

$$\tau_y(x) = \sigma_{\sigma_x(y)}^{-1}(x), \quad \sigma_x(y) = \tau_{\tau_y(x)}^{-1}(y) \tag{2.2}$$

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 $\{\tau_x : x \in X\}$.

Definition 2.57. A *cycle set* is a pair $(X, \cdot)$, where X is a non-empty set provided with a binary operation $X \times X \to X$, $(x, y) \mapsto x \cdot y$, such that

$$(x \cdot y) \cdot (x \cdot z) = (y \cdot x) \cdot (y \cdot z) \tag{2.3}$$

eq:cycle_set

holds for all $x, y, z \in X$ and each map $\varphi_x \colon X \to X$, $y \mapsto x \cdot y$, is bijective. A cycle set $(X, \cdot)$ is said to be *non-degenerate* if the map $X \to X$, $x \mapsto x \cdot x$, is bijective.

Definition 2.58. Let X and Z be cycle sets. A *homomorphism* between the cycle sets X and Z is a map $f \colon X \to Z$ such that $f(x \cdot y) = f(x) \cdot f(y)$ for all $x, y \in X$. An *isomorphism* of cycle sets is a bijective homomorphism of cycle sets.

Cycle sets and cycle set homomorphisms form a category. It is possible to prove that the category of solutions is equivalent to the category of cycle sets, see Exercise 2.1.

thm:CS **Theorem 2.59.** *There exists a bijective correspondence between non-isomorphic involutive solutions and non-isomorphic non-degenerate cycle sets.*

For the readers who are not familiar with the above-mentioned result, the bijective correspondence is given by

$$r(x,y) = (x * y, (x * y) \cdot x),$$

where $x * y = z$ if and only if $x \cdot z = y$. We leave the proof for the reader, see Exercise 2.4. However, we will prove a more general result in Theorem 3.14.

Theorem 2.59 can be used to construct and enumerate small involutive solutions [2]. Table 2.1 shows the number of non-isomorphic involutive solutions of size ≤ 10. For size ≤ 7 the numbers of Table 2.1 coincide with those in [32] but differ by two for $n = 8$, as two solutions of size eight are missing in [32].

Table 2.1: Involutive solutions of size ≤ 10.

tab:IYB

n	2	3	4	5	6	7	8	9	10
solutions	2	5	23	88	595	3456	34530	321931	4895272

prob:cycle_sets **2.1.** Prove that the category of non-degenerate cycle sets and the category of solutions are equivalent.

prob:Rump **2.2.** Prove Proposition 2.55.

2.3. If X is a cycle set, then $x \cdot (y \cdot y) = ((y * x) \cdot y) \cdot ((y * x) \cdot y)$, where $y * x = z$ if and only if $y \cdot z = x$.

prob:CS **2.4.** Prove Theorem 2.59.

Open problems

prob:Koethe **Open problem 2.1 (Köthe).** Let R be a ring. Is the sum of two arbitrary nil left ideals of R is nil?

Open problem 2.2. Construct and enumerate involutive solutions of size 11.

Open problem 2.3. Estimate the number of solutions of size n for $n \to \infty$.

Notes

The material on non-commutative ring theory is standard, see for example [12]. Radical rings were introduced by Jacobson in [41]. Nil rings were used by Zelmanov in his solution to Burnside's problem, see for example [70].

Open problem 2.1 is the well-known Köthe's conjecture. The conjecture was first formulated in 1930, see [44]. It is known to be true in several cases. In full generality, the problem is still open. In [45] Krempa proved that the following statements are equivalent:

1) Köthe's conjecture is true.
2) If R is a nil ring, then $R[X]$ is a radical ring.
3) If R is a nil ring, then $M_2(R)$ is a nil ring.
4) Let $n \geq 2$. If R is a nil ring, then $M_n(R)$ is a nil ring.

In 1956 Amitsur formulated the following conjecture, see for example [4]: If R is a nil ring, then $R[X]$ is a nil ring. In [58] Smoktunowicz found a counterexample to Amitsur's conjecture. This counterexample suggests that Köthe's conjecture might be false. A simplification of Smoktunowicz's example appears in [50]. See [59, 60] for more information on Köthe's conjecture and related topics.

Rump introduced cycle sets in [55]. The bijective correspondence of Theorem 2.59 was also proved by Rump in [55]. A similar result can be found in [32, Proposition 2.2].

The numbers of Table 2.1 were computed in [2] using a combination of [33] and constraint programming techniques. The algorithm is based on an idea of Plemmons [52], originally conceived to construct non-isomorphic semigroups.

Chapter 3
Racks

A

defn:rack **Definition 3.1.** A *rack* is a pair $(X,\triangleright)$, where X is a non-empty set and $X\times X\to X$, $(x,y)\mapsto x\triangleright y$, is a binary operation on X such that the maps $\rho_y\colon X\to X$, $x\mapsto x\triangleleft y$, are bijective for all $y\in X$, and

$$(x\triangleleft y)\triangleleft z=(x\triangleleft z)\triangleleft(y\triangleleft z) \tag{3.1}$$ eq:rack

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

Racks are used in low-dimensional topology [30], singularities [13] and in the classification of finite-dimensional pointed Hopf algebras [5].

Example 3.2. Let X be a set. Then $x\triangleleft y=x$ turns X into a rack. This is the *trivial rack* on X.

Example 3.3. Let $X=\mathbb{Z}/n$. Then $x\triangleleft y=2y-x$ turns X into a rack. This is the *dihedral rack* of size n.

Example 3.4. Let A be an abelian group and $f\in\mathrm{Aut}(A)$. Then

$$x\triangleleft y=(\mathrm{id}-f)(y)+f(x)$$

turns A into a rack. These racks are known as the *Alexander racks*.

Definition 3.5. Let X and Z be racks. A *rack homomorphism* between the racks X and Z is a map $f\colon X\to Z$ such that $f(x\triangleleft y)=f(x)\triangleleft f(y)$ for all $x,y\in X$. An *isomorphism* of racks is a bijective rack homomorphism.

For $n\in\mathbb{N}$, let $r(n)$ be the number of isomorphism classes of racks of size n. Some values of $r(n)$ appear in Table 3.1, see for example [67].

Table 3.1: Enumeration of non-isomorphic racks.

tab:racks

n	2	3	4	5	6	7	8	9	10	11	12	13
$r(n)$	2	6	19	74	353	2080	16023	159526	2093244	36265070	836395102	25794670618

pro:Venkov

Proposition 3.6. *Let X be a non-empty set and $X\times X\to X$, $(x,y)\mapsto x\triangleleft y$ be a binary operation on X. Then $r(x,y)=(y,x\triangleleft y)$ is a solution if and only if $(X,\triangleleft)$ is a rack.*

Proof. The map r satisfies $(r\times\mathrm{id})(\mathrm{id}\times r)(r\times\mathrm{id})=(\mathrm{id}\times r)(r\times\mathrm{id})(\mathrm{id}\times r)$ if and only if (3.1) holds for all $x,y,z\in X$. The solution (X,r) is non-degenerate if the maps $X\to X$, $x\mapsto x\triangleleft y$, are bijective. $\square$

The connection between racks and solutions goes deeper than the phenomenon appearing in Proposition 3.6.

pro:derived

Proposition 3.7. *Let (X,r) be a solution. Then*

$$x\triangleleft y=\sigma_y\tau_{\sigma_x^{-1}(y)}(x)=\sigma_y\widehat{\sigma}_y^{-1}(x) \tag{3.2}$$

eq:derived

turns X into a rack and each σ_x is a rack homomorphism. Moreover, (X,r) is involutive if and only if the rack $(X,\triangleleft)$ is trivial.

Proof. Since $r(x,\sigma_x^{-1}(y))=(y,\tau_{\sigma_x^{-1}(y)}(x))$, it follows that $\widehat{\sigma}_y^{-1}(x)=\tau_{\sigma_x^{-1}(y)}(x)$ for all $x,y\in X$. Hence the second equality of (3.2) holds.

To prove that each τ_z is a rack homomorphism it is enough to show that

$$\sigma_x(y)\triangleleft\sigma_x\sigma_y(z)=\sigma_x(y\triangleleft\sigma_y(z))$$

for all $x,y\in X$. Write $r(x,y)=(u,v)$. On the one hand, by Lemma 1.3,

$$\sigma_x(y)\triangleleft\sigma_x\sigma_y(z)=u\triangleleft\sigma_u\sigma_v(z)=\sigma_{\sigma_u\sigma_v(z)}\tau_{\sigma_{\tau_y(x)}(z)}\sigma_x(y)=\sigma_{\sigma_x\sigma_y(z)}\sigma_{\tau_{\sigma_y(z)}(x)}\tau_z(y).$$

On the other hand,

$$\sigma_x(y\triangleleft\sigma_y(z))=\sigma_x\sigma_{\sigma_y(z)\tau_z(y)}=\sigma_{\sigma_x\sigma_y(z)}\sigma_{\tau_{\sigma_y(z)}(x)}\tau_z(y).$$

By Proposition 3.6, in order to prove that $(X,\triangleright)$ is a rack it is enough to show that $r(x,y)=(y,x\triangleleft y)$ satisfies the YBE. For that purpose, we demonstrate that the map $J\colon X^3\to X^3$, $J(x,y,z)=(x,\sigma_x(y),\sigma_x\sigma_y(z))$ is invertible and satisfies

$$(\mathrm{id}\times s)\circ J=J\circ(\mathrm{id}\times r),\quad (s\times\mathrm{id})\circ J=J\circ(r\times\mathrm{id}).$$

The map $(x,y,z)\mapsto(x,\sigma_x^{-1}(y),\sigma_{\sigma_x^{-1}(y)}^{-1}\sigma_x^{-1}(z))$ is the inverse of J.

Since σ_x is a rack homomorphism,

$$\sigma_x(y)\triangleleft\sigma_x\sigma_y(z)=\sigma_x(y\triangleleft\sigma_y(z))=\sigma_x\sigma_{\sigma_y(z)}\tau_{\sigma_y^{-1}\sigma_y(z)}(y)=\sigma_x\sigma_{\sigma_y(z)}\tau_z(y)$$

Then it follows that

$$\begin{aligned}(\mathrm{id}\times s)J(x,y,z) &= (\mathrm{id}\times s)(x,\sigma_x(y),\sigma_x\sigma_y(z))\\ &= (x,\sigma_x\sigma_y(z),\sigma_x(y)\triangleleft\sigma_x\sigma_y(z))\\ &= (x,\sigma_x\sigma_y(z),\sigma_x\sigma_{\sigma_y(z)}\tau_z(y))\\ &= J(x,\sigma_y(z),\tau_z(y))\\ &= J(\mathrm{id}\times r)(x,y,z).\end{aligned}$$

Similarly one proves that $(s\times\mathrm{id})\circ J = J\circ(r\times\mathrm{id})$. This implies that (X,s) is a solution and hence $(X,\triangleleft)$ is a rack by Proposition 3.6.

If (X,r) is involutive, then $x\triangleleft\sigma_x(y)=\sigma_{\sigma_x(y)}\tau_y(x)=x$ by (2.2). Conversely, if $x\triangleleft y=x$ for all $x,y\in X$, then r is involutive, as

$$r^2(x,\sigma_x^{-1}(y)) = r(y,\sigma_y^{-1}(x)) = (x,\sigma_x^{-1}(y)). \qquad \square$$

The rack constructed in Proposition 3.7 is known as the *derived solution* of (X,r). There is a dual version of the derived rack:

pro:derived_dual

Proposition 3.8. *Let (X,r) be a solution. Then*

$$x\blacktriangleleft y = \tau_y\sigma_{\tau_x^{-1}(y)}(x) = \tau_y\widehat{\tau}_y^{-1}(x)$$

turns X into a rack and each τ_x is a rack homomorphism.

Proof. Since (X,r) is a solution, then so is (X,r_0), where $r_0(x,y)=(\tau_x(y),\sigma_y(x))$. Then the claim follows from Proposition 3.8 applied to the solution (X,r_0). $\square$

In general, the racks constructed in Propositions 3.7 and 3.8 are different:

Example 3.9. Let $X=\{1,\dots,5\}$ and (X,r) be the solution given by

$$\begin{aligned}&\sigma_1=\mathrm{id}, && \sigma_2=\mathrm{id}, && \sigma_3=\mathrm{id}, && \sigma_4=(13)(45), && \sigma_5=(12)(45),\\ &\tau_1=\mathrm{id}, && \tau_2=\mathrm{id}, && \tau_3=\mathrm{id}, && \tau_4=(23)(45), && \tau_5=(23)(45).\end{aligned}$$

On the one hand the derived rack of (X,r) is given by the permutations

$$\sigma_1\widehat{\sigma}_1^{-1}=\sigma_2\widehat{\sigma}_2^{-1}=\sigma_3\widehat{\sigma}_3^{-1}=\mathrm{id},\qquad \sigma_4\widehat{\sigma}_4^{-1}=(132),\qquad \sigma_5\widehat{\sigma}_5^{-1}=(123).$$

On the other hand, the dual derived rack by

$$\tau_1\widehat{\tau}_1^{-1}=\tau_2\widehat{\tau}_2^{-1}=\tau_3\widehat{\tau}_3^{-1}=\mathrm{id},\qquad \tau_4\widehat{\tau}_4^{-1}=(123),\qquad \tau_5\widehat{\tau}_5^{-1}=(132).$$

We now prove that the racks of Propositions 3.7 and 3.8 are isomorphic. We shall need a lemma.

lem:T_invertible

Lemma 3.10. *Let (X,r) be a solution. The map $T\colon X\to X$, $x\mapsto\sigma_x^{-1}(x)$, is invertible with inverse $U\colon X\to X$, $x\mapsto\tau_x^{-1}(x\blacktriangleleft x)$.*

Proof. Let $x \in X$ and $y = U(x) = \tau_x^{-1}(x \blacktriangleleft x)$. Then $\tau_x(y) = x \blacktriangleleft x = \tau_x \widehat{\tau}_x^{-1}(x)$ and hence $y = \widehat{\tau}_x^{-1}(x)$. Then $\widehat{\tau}_x(y) = x$ and

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

where $z \in X$ is such that $\sigma_z(x) = y$. By Lemma 1.3, $\sigma_y = \sigma_z$. Then it follows that $x = \sigma_y^{-1}(y) = T(y)$. Therefore $y = U(x) = U(T(y))$.

To prove that $T(U(x)) = x$, first note that

$$r(\tau_x^{-1}(x), x) = (\sigma_{\tau_x^{-1}(x)}(x), x)$$

and Lemma 1.3 imply that $\sigma_{\tau_x^{-1}(x)} = \sigma_{\sigma_{\tau_x^{-1}(x)}(x)}$. Now

$$\begin{aligned} T(U(x)) &= T(\tau_x^{-1}(x \blacktriangleleft x)) = T(\sigma_{\tau_x^{-1}(x)}(x)) \\ &= \sigma^{-1}_{\sigma_{\tau_x^{-1}(x)}(x)} \sigma_{\tau_x^{-1}(x)}(x) = \sigma^{-1}_{\tau_x^{-1}(x)} \sigma_{\tau_x^{-1}(x)}(x) = x. \end{aligned}$$

□

There is version of Proposition 2.56 for arbitrary solutions. A similar result appears in Exercise 3.3.

Proposition 3.11. *Let (X,r) be a solution. Then $T \colon X \to X$, $x \mapsto \tau_x^{-1}(x)$, is a bijective map such that*

$$T \circ \tau_y = \widehat{\sigma}_y^{-1} \circ T, \quad T \circ \widehat{\tau}_y = \sigma_y^{-1} \circ T$$

and $T(x \blacktriangleleft y) = T(x) \triangleleft T(y)$ for all $x, y \in X$.

Proof. Lemma 3.10 proves that T is bijective. We now compute

$$\begin{aligned} T\tau_y(x) &= \sigma^{-1}_{\tau_y(x)} \tau_y(x) = \sigma^{-1}_{\tau_y(x)} \sigma^{-1}_{\sigma_x(y)} \sigma_{\sigma_x(y)} \tau_y(x) \\ &= \sigma_y^{-1} \sigma_x^{-1} \sigma_{\sigma_x(y)} \tau_y(x) = \sigma_y^{-1} \sigma_x^{-1}(x \triangleleft \sigma_x(y)) = \sigma_y^{-1}(T(y) \triangleleft y) = \widehat{\sigma}_y^{-1} T(x). \end{aligned}$$

Since $\widehat{\tau}_y(x) = \sigma^{-1}_{\widehat{\sigma}_x(y)}(x)$, Lemma 1.3 implies that

$$T\widehat{\tau}_y(x) = \sigma^{-1}_{\widehat{\tau}_y(x)} \widehat{\tau}_y(x) = \sigma^{-1}_{\widehat{\tau}_y(x)} \sigma^{-1}_{\widehat{\sigma}_x(y)} = \sigma_y^{-1} \sigma_x^{-1}(x) = \sigma_y^{-1} T(x).$$

These formulas imply that

$$T \circ \tau_y \circ \widehat{\tau}_y^{-1} = \widehat{\sigma}_y^{-1} \circ T \circ \widehat{\tau}_y^{-1} = \widehat{\sigma}_y^{-1} \circ \sigma_y \circ T. \tag{3.3}$$

eq:T_rack

We evaluate Equality (3.3) on X. On the one hand, $T(x \blacktriangleleft y) = T\sigma_x \widehat{\sigma}_x^{-1}(y)$. On the other hand,

$$\widehat{\sigma}_y^{-1} \sigma_y T(x) = \sigma_y^{-1} \sigma_y \widehat{\sigma}_y^{-1} \sigma_y T(x) = \sigma_y^{-1}(\sigma_y T(x) \triangleleft y) = T(x) \triangleleft T(y).$$

□

As it happens in the involutive case, there is a nice combinatorial structure that describes a solution.

defn:skewCS

Definition 3.12. A *skew cycle set* is a triple $(X, \triangleleft, \cdot)$, where X is a non-empty set, $(X, \triangleleft)$ is a rack and $X \times X \to X$, $(x,y) \mapsto x \cdot y$, is a binary operation on X such that the maps $X \to X$, $y \mapsto x \cdot y$, are bijective rack homomorphisms, and

$$(x \cdot y) \cdot (x \cdot z) = (y \cdot (x \triangleleft y)) \cdot (y \cdot z) \tag{3.4}$$

eq:skew_CS

for all $x, y, z \in X$. A skew cycle set $(X, \triangleleft, \cdot)$ is said to be non-degenerate if the map $X \times X$, $x \mapsto x \cdot x$, is bijective.

FIXME

Definition 3.13. Let X and Z be skew cycle sets. A *homomorphism* between the cycle sets X and Z is a map $f \colon X \to Z$ such that $f(x \cdot y) = f(x) \cdot f(y)$ for all $x, y \in X$. An *isomorphism* of cycle sets is a bijective homomorphism of cycle sets.

Cycle sets and cycle set homomorphisms form a category. It is possible to prove that the category of solutions is equivalent to the category of cycle sets, see Exercise 2.1.

Theorem 2.59 can be generalized to arbitrary solutions.

thm:skewCS

Theorem 3.14. *There exists a bijective correspondence between solutions and non-degenerate skew cycle sets.*

Proof. Let (X, r) be a solution and $(X, \triangleleft)$ its derived rack. We will prove that the operation $x \cdot y = \sigma_x^{-1}(y)$ turns $(X, \triangleleft)$ into a skew cycle set. By Proposition 3.7, the maps $X \to X$, $y \mapsto x \cdot y$, are bijective rack homomorphisms.

On the one hand, since $r(x, \sigma_x^{-1}(y)) = (y, \tau_{\sigma_x^{-1}(y)}(x))$,

$$\begin{aligned}(x \cdot y) \cdot (x \cdot z) &= \sigma_x^{-1}(y) \cdot \sigma_x^{-1}(z) = \sigma^{-1}_{\sigma_x^{-1}(y)} \sigma_x^{-1}(z)\\ &= \left(\sigma_x \circ \sigma_{\sigma_x^{-1}(y)}\right)^{-1}(z) = \left(\sigma_y \circ \sigma_{\tau_{\sigma_x^{-1}(y)}(x)}\right)^{-1}(z).\end{aligned}$$

On the other hand,

$$\begin{aligned}(y \cdot (x \triangleleft y)) \cdot (y \cdot z) &= \sigma_y^{-1}(\sigma_y \tau_{\sigma_x^{-1}(y)}(x)) \cdot \sigma_y^{-1}(z)\\ &= \sigma^{-1}_{\tau_{\sigma_x^{-1}(y)}(x)} \sigma_y^{-1}(z) = \left(\sigma_y \circ \sigma_{\tau_{\sigma_x^{-1}(y)}(x)}\right)^{-1}(z).\end{aligned}$$

Now we prove the converse statement. For $x, y \in X$ let

$$\sigma_x(y) = x * y, \quad \tau_y(x) = \sigma^{-1}_{\sigma_x(y)}(x \triangleleft \sigma_x(y)),$$

where $x * y = z$ if and only if $x \cdot z = y$. Since X is a skew cycle set, each σ_x is bijective. Let us prove that the τ_x are bijective. Equality (3.4) with $y = \sigma_x(z)$ implies that

$$\sigma_z^{-1} \sigma_x^{-1} = \sigma^{-1}_{\sigma_x^{-1}(y)} \sigma_x^{-1} = \sigma^{-1}_{\sigma_y^{-1}(x \triangleleft y)} \sigma_y^{-1} = \sigma^{-1}_{\sigma^{-1}_{\sigma_x(z)}(x \triangleleft \sigma_x(z))} \sigma^{-1}_{\sigma_x(z)} = \sigma^{-1}_{\tau_z(x)} \sigma^{-1}_{\sigma_x(z)}$$

for all $x,z \in X$. Since each σ_x is a rack homomorphism,

$$\tau_y(x) = \sigma^{-1}_{\sigma_x(y)}(x \triangleleft \sigma_x(y)) = \sigma^{-1}_{\sigma_x(y)}\sigma_x(\sigma_x^{-1}(x) \triangleleft y) = \sigma_{\tau_y(x)}\sigma_y^{-1}(\sigma_x^{-1}(x) \triangleleft y).$$

Therefore $T \circ \tau_y = \sigma_y^{-1} \circ \rho_y \circ T$, where $T\colon X \to X$, $T(x) = x \cdot x$ and $\rho_y\colon X \to X$, $\rho_y(x) = x \triangleleft y$ are bijective maps. In particular, τ_y is bijective for all $y \in X$.

Now we prove that... $\boxed{\text{solution?}}$

$\boxed{\text{invertible?}}$ □

Theorem 3.14 can be used to construct small solutions, see Table 3.2.

Table 3.2: Enumeration of non-involutive solutions.

tab:non_involutive

n	2	3	4	5	6	7	8
$s(n)$	2	21	253	3519	100071	4602720	422449480

B

An interesting family of racks is that that of quandles. A **quandle** is a rack $(X,\triangleleft)$ such that $x \triangleleft x = x$ for all $x \in X$.

Exercises

prob:xx **3.1.** Prove that $x \triangleright x = x \blacktriangleright x$ for all $x \in X$.

prob:tau_hat **3.2.** Prove that $\widehat{\tau}_x(y \triangleright z) = \widehat{\tau}_x(y) \triangleright \widehat{\tau}_x(z)$ for all $x,y,z \in X$.

prob:variationT **3.3.** Let (X,r) be a solution and let $(X,\triangleright)$ be its derived rack. Prove that

$$T\sigma_x(y) = \tau_x^{-1}(x \triangleright T(y))$$

for all $x \in X$, where $T\colon X \to X$, $T(y) = \tau_y^{-1}(y)$.

prob:guitar **3.4.** Let (X,r) be a solution and $(X,\triangleright)$ its derived rack. Let $T_2(x,y) = (\tau_y(x),y)$ and $T_{n+1} = Q_n \circ (T_n \times \mathrm{id})$ for $n \geq 2$, where

$$Q_n(x_1,\dots,x_{n+1}) = (\tau_{x_{n+1}}(x_1),\dots,\tau_{x_{n+1}}(x_n),x_{n+1}).$$

Prove that $T_n \circ r_{i,i+1} = s_{i,i+1} \circ T_n$ for all $n \geq 2$ and $i \in \{1,\dots,n-1\}$.

Open problems

problem:racks14 **Open problem 3.1.** Enumerate isomorphism classes of racks of size 14.

Open problem 3.2. Enumerate non-involutive solutions of size ≥ 9.

Notes

A particular family of racks turns out to be useful in combinatorial know theory. A quandle is a rack $(X, \triangleleft)$ such that $x \triangleleft x = x$ for all $x \in X$.

In [29], Drinfeld attributes Proposition 3.6 to Venkov.

There are several papers on the enumeration of isomorphic classes of finite racks [6, 11, 38]. Estimations on the number of finite racks of size n appear in [11].

The numbers of Table 3.2 were computed using Theorem 3.14 essentially with the same technique used to construct involutive solutions [2]. The construction of non-involutive solutions of size 9 seems to be feasible with these methods. However, it should be noted that a huge number of solutions is expected.

Exercises 3.1 and 3.2 appear in [47].

The map J of Exercise 3.4 is known as the *guitar map*. It was first considered by Etingof, Schedler and Soloviev in [32] for involutive solutions. The construction was extended to non-involutive solutions by Soloviev in [64] and Lu, Yan and Zhu in [48]. In [28] Dehornoy used the inverse of the guitar map to develop his right-cyclic calculus and to obtain short proofs for results on the structure group of involutive solutions. In [5] Andruskiewitsch and Graña use the guitar map to study certain isomorphisms of Nichols algebras. A particular case of the guitar map also appears in the work of Przytycki [54].

The derived rack of a solution was first defined in the work of Soloviev [64]. Most of the properties of the derived racks mentioned in this chapter were proved in [47].

Problem 3.1 appears in [67].

Chapter 4
Braces

braces

A

By convention, an additive group A will be a (not necessarily abelian) group with 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 $-a$.

def:brace **Definition 4.1.** A *brace* is a triple $(A,+,\circ)$, where $(A,+)$ and $(A,\circ)$ are (not necessarily abelian) groups and

$$a \circ (b+c) = (a \circ b) - a + (a \circ c) \tag{4.1}$$ eq:compatibility

holds for all $a,b,c \in A$, where $-a$ denotes the inverse of a with respect to the group structure given by $(a,b) \mapsto a+b$. 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 a left brace. Right braces are defined similarly, one needs to replace (4.1) by

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

There is a bijective correspondence between left and right braces, see Exercise 4.1. For that reason, a brace will always mean a left brace.

Definition 4.2. Let $\mathscr{X}$ be a property of groups. A brace A is said to be of $\mathscr{X}$-type if its additive group belongs to $\mathscr{X}$.

One particularly interesting families of braces is the family of *braces of abelian type*, that is braces with abelian additive group. Braces of abelian type were introduced by Rump in [56] to study involutive solutions to the Yang–Baxter equation. In the literature, braces of abelian type are called *left braces*.

exa:trivial **Example 4.3.** 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 4.4.** 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.

exa:sd **Example 4.5.** Let A and M be additive groups and let $\alpha\colon A\to \operatorname{Aut}(M)$ 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:s3c6 **Example 4.6.** Let $A=\mathbb{S}_3$ be the symmetric group in three letters. Write A as an additive group. Let $\lambda: A\to\mathbb{S}_A$ be the map given by

$$\begin{aligned}&\lambda_{\mathrm{id}}=\lambda_{(123)}=\lambda_{(132)}=\mathrm{id},\\ &\lambda_{(12)}=\lambda_{(23)}=\lambda_{(13)}=\text{conjugation by }(23).\end{aligned}$$

It is easy to check that $\lambda_{a+\lambda_a(b)}=\lambda_a\lambda_b$ for all $a,b\in A$. Hence A is a brace by Exercise 4.5. Since the transposition (12) has order six in the multiplicative group of A, it follows that the additive group of A is isomorphic to $\mathbb{S}_3$ and the multiplicative group of A is isomorphic to the cyclic group of order six.

The following example is motivated by the paper [69].

exa:WX **Example 4.7.** Let A be an additive group and B and C be subgroups of A such that A admits an *exact factorization* as $A=B+C$. 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 the direct product $B\times C$ into the set A. For $a=b+c\in A$ 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 examples of the previous construction.

exa:QR

Example 4.8. Let $n \in \mathbb{N}$. The group $\mathbf{GL}_n(\mathbb{C})$ admits an exact factorization through the subgroups $U(n)$ and $T(n)$, where $U(n)$ 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 extensions, see [15, Corollary 1.1].

exa:a5a4c5

Example 4.9. 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 $\mathbb{A}_4 \times C_5$.

exa:PSL27S4C7

Example 4.10. The simple group $\mathbf{PSL}_2(7)$ admits an exact factorization through the subgroups $A \simeq \mathbb{S}_4$ and $B \simeq C_7$. There exists a brace with additive group isomorphic to $\mathbf{PSL}_2(7)$ and multiplicative group isomorphic to $\mathbb{S}_4 \times C_7$.

lem:basic

Lemma 4.11. *Let A be a brace. Then the following properties hold:*

1) $0 = 1$.
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* $a, b, c \in A$.

Proof. The first claim follows from the compatibility condition (4.1) with $c = 1$. To prove the second claim let $d = b + c$. Then (4.1) becomes

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

and the claim follows. The third claim is proved similarly. $\square$

pro:lambda

Proposition 4.12. *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 bijective. Moreover, the map $\lambda \colon (A, \circ) \to \operatorname{Aut}(A, +)$, $a \mapsto \lambda_a$, is a group homomorphism.

Proof. The inverse of λ 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

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

To prove that λ is a group homomorphism, we use Lemma 4.11 to obtain

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

If A is a brace, the map λ is the previous proposition yields a left action from $(A,\circ)$ on $(A,+)$ by automorphisms. There is also a right action $(A,\circ)$ on $(A,+)$ by automorphisms:

pro:mu **Proposition 4.13.** *Let A be a brace. For each $a\in A$, the map*

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

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 $a,b\in A$.

Proof. Let $a,b,c\in A$. To prove that μ is a brace anti-homorphism, we compute

$$\mu_{b\circ a}(c)=\lambda_c((b\circ a)'\circ c\circ b\circ a)$$

and

$$\mu_a\mu_b(c)=\mu_a(\lambda_c(b)'\circ c\circ b)=\lambda_{\lambda_c(b)'\circ c\circ b}(a)'\circ(\lambda_c((b\circ a)'\circ c\circ b)).$$

Using the formulas (4.2),

$$\begin{aligned}\lambda_c(b\circ a)'&=\lambda_c(b+\lambda_b(a))=(\lambda_c(b)+\lambda_{c\circ b}(a)')\\&=(\lambda_c(b)\circ\lambda^{-1}_{\lambda_c(b)}\lambda_{c\circ b}(a))'=\lambda_{\lambda_c(b)'\circ c\circ b}(a)'\circ\lambda_c(b)',\end{aligned}$$

which proves that μ is an anti-homomorphism.

To compute the inverse of μ_b we proceed as follows. Since $a'\circ(-a)=2a$ by Lemma 4.11,

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

From this one immediately obtains that $\mu_b^{-1}(a)=(b\circ a'-b)'$. $\square$

Let A be a brace. The previous proposition implies that

$$a\circ b=a+\lambda_a(b),\qquad a+b=a\circ\lambda_a^{-1}(b),\qquad \lambda_a(a')=-a \tag{4.2}$$ 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:

$$a*(b+c)=a*b+b+a*c-b, \tag{4.3}$$
$$(a\circ b)*c=(a*(b*c))+b*c+a*c. \tag{4.4}$$

These last two identities are similar to the usual *commutator identities*.

Definition 4.14. A *homomorphism* between two braces A and B is a group homomorphism $f\colon A\to B$ such that $f\lambda_a=\lambda_{f(a)}f$ for all $a\in A$. The *kernel* of f is

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

Braces and brace homomorphisms form a category.

Definition 4.15. A brace A is said to be a *two-sided* if

$$(a+b)\circ c = a\circ c - c + b\circ c \tag{4.5}$$

eq:right_compatibility

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

If A is a two-sided brace, then

$$a\circ(-b) = a - a\circ b + a, \qquad (-a)\circ b = b - a\circ b + b \tag{4.6}$$

eq:2sided

hold for all $a,b \in A$. The first equality holds for every brace and follows from Lemma 4.11. The second equality follows from (4.5).

Example 4.16. Any brace with abelian multiplicative group is two-sided.

Example 4.17. Let $n \in \mathbb{N}$ be such that $n = p_1^{a_1}\cdots p_k^{a_k}$, where the p_j are distinct primes, all $a_j \in \{0,1,2\}$ and $p_i^m \not\equiv 1 \bmod p_j$ for all i,j,m with $1 \leq m \leq a_i$. Then every brace of size n is a two-sided brace of abelian type, since every group of order n is abelian, see for example [51].

Two-sided braces of abelian type form an interesting family of rings without unit.
Braces are a far reaching generalizations of radical rings. The following result was proved by Rump in [56].

thm:radical

Theorem 4.18. *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

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

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

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

Similarly, since A is two-sided ones proves $(a+b)c = ac + bc$. It remains to show that the multiplication is associative. On the one hand, using the first equality of (4.6) and the brace compatibility condition, we write

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

since the group $(A,+)$ is abelian. On the other hand, the second equality of (4.6) and Equality (4.5) imply that

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

It then follows that the multiplication 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 brace is said to be *associative* if the operation $(x,y)\mapsto x*y=\lambda_x(y)-y$ is associative. In [19, Question 2.1(2)], Cedó, Gateva–Ivanova and Smoktunowicz asked if associative braces of abelian type are always radical rings. To answer this question, we need some lemmas.

Lemma 4.19. *If A is an associative brace of abelian type, then $(-a)*b=-(a*b)$ holds for all $a,b\in A$. In particular, $(-a)\circ b=2b-(a\circ b)$ for all $a,b\in A$.*

Proof. The associativity implies that

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

and therefore $(-a)*b=-(a*b)$. From this the claim follows. □

If A is a brace of abelian type, then one proves by induction that

$$a\circ\left(\sum_{i=1}^n b_i-\sum_{j=1}^m c_j\right)=\sum_{i=1}^n a\circ b_i-\sum_{j=1}^m a\circ c_j+(m-n+1)a \tag{4.7}$$ eq:Lau

holds for all $a,b,c\in A$, see Exercise 4.7.

thm:Lau **Theorem 4.20.** *If A is an associative brace of abelian type, then A is a radical ring.*

Proof. We need to prove that the right compatibility condition holds. Since A is associative, $(a*b)*c=a*(b*c)$ for all $a,b,c\in A$. Write the associativity condition between $a,b,c\in A$ as

$$(a\circ b-a-b)\circ c-(a\circ b-a-b)-c=a\circ(b\circ c-b-c)-a-(b\circ c-b-c),$$

which is equivalent to

$$a' \circ ((a \circ b - a - b) \circ c - a \circ b) = a' \circ (a \circ (b \circ c - b - c) - a - a - b \circ c + 2c).$$

By using the formula (4.7) with $n = 1$ and $m = 2$ in the right hand side and with $n = m = 3$ in the left hand side,

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

Now (4.7) with $n = 2$ and $m = 1$ implies that the associativity of A is equivalent to

$$(b + a' \circ (-b)) \circ c + c = b \circ c + a' \circ (-b) \circ c. \tag{4.8}$$ eq:asociatividad

Let $b, c \in A$. If $d \in A$, then there exists $a \in a$ such that $d = a' \circ (-b)$. Equality (4.8) implies that

$$(b + d) \circ c + c = b \circ c + d \circ c. \qquad \square$$

The previous result is not true if the brace is not of abelian type.

Now we show a brace that is not two-sided:

Example 4.21.

In Proposition 2.55 we used radical rings to produce examples of solutions. A natural question arises: Does one need radical rings? Surprisingly, radical rings are just the tip of the iceberg.

thm:YB **Theorem 4.22.** *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.

Proof. By Theorem 1.11, 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 Proposition 4.12 and for the right action we use Proposition 4.13. $\square$

In Theorem 4.22 it is possible to prove that the solution is involutive if and only if the additive group of the brace is abelian. The next result generalizes this fact. We shall need a lemma.

lem:|r| **Lemma 4.23.** *Let A be a brace and r be its associated solution. Then*

$$\begin{aligned} r^{2n}(a, b) = (&-n(a \circ b) + a + n(a \circ b), \\ &(-n(a \circ b) + a + n(a \circ b))' \circ a \circ b), \end{aligned} \tag{4.9}$$ eq:r^2n

$$\begin{aligned} r^{2n+1}(a, b) = (&-n(a \circ b) - a + (n+1)(a \circ b), \\ &(-n(a \circ b) - a + (n+1)(a \circ b))' \circ a \circ b), \end{aligned} \tag{4.10}$$ 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. It suffices to prove (4.9) and (4.10). We proceed by induction on n. The case $n = 0$ is trivial for (4.9) and (4.10). Assume that the claim holds for some $n > 0$. If n is even, by applying the map r to Equation (4.9) we obtain that

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

Thus Equation (4.10) holds. If n is odd, a similar argument shows that (4.9) holds. The other claims follow easily from Equations (4.9) and (4.10). □

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

thm:|r|

Theorem 4.24. *Let A be a finite brace with more than one element and let G be the additive group of A. If r is the solution associated with A, then r has order* $2\exp(G/Z(G))$.

Proof. Let n be such that r has odd order, say $r^{2n+1} = \mathrm{id}$. By applying Lemma 4.23 one obtains that $-a + (n+1)(a \circ b) = n(a \circ b) + a$ for all $a, b \in A$. In particular, if $b = 0$, then $a = 0$, a contradiction. Therefore we may assume that the order of the permutation r is $2n$, where

$$n = \min\{k : kb + a = a + kb \text{ for all } a, b \in A\}.$$

Now one computes

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

An inmmediate consequence:

Corollary 4.25. *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.*

4B

Definition 4.26. 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 4.27. 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 $(A, +)$.

Proposition 4.28. *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 $x'=-\lambda_x(x)\in I$. $\square$

Example 4.29. Let A be a brace. Then

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

is a left ideal of A.

Definition 4.30. An *ideal* of A is a strong left ideal I of A such that $(I,\circ)$ is a normal subgroup of $(A,\circ)$.

In general

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

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

Example 4.31. 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

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

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

Example 4.32. Let $f\colon A\to B$ be a brace homomorphism. Then $\ker f$ is an ideal of A.

Let I and J be ideals of a A. Then $I\cap J$ is an ideal of A, see Exercise 4.9. 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 4.33. *Let A be a brace and let I and J be ideals of A. Then $I+J$ is an ideal of A.*

Proof. Let $a\in A$, $u\in I$ and $v\in J$. Then $\lambda_a(u+v)\in I+J$ and hence it follows that $\lambda_a(I+J)\subseteq I+J$. Moreover,

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

This formula implies that

$$a\circ(u+v)\circ a'=a+\lambda_a((u+v)+(u+v)*a')-a\in I+J.$$

Thus it follows that $a\circ(I+J)\circ a'\subseteq I+J$.

Finally $I+J$ is a normal subgroup of $(A,+)$ since

$$a+\sum_k (u_k+v_k)-a=\sum_k ((a+u_k-a)+(a+v_k-a))\in I+J$$

whenever $u_k \in I$ and $v_k \in J$ for all k. □

Definition 4.34. Let A be a brace. The subset $\mathrm{Soc}(A)=\ker\lambda\cap Z(A,+)$ is the *socle* of A.

lem:socle

Lemma 4.35. *Let A be a brace and $a\in\mathrm{Soc}(A)$. Then*

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

both hold for all $b\in A$.

Proof. Let $b\in A$. Since $b'\circ(b\circ a+b)=a-b'$ and $b'\circ(b+b\circ a)=-b'+a$, the first claim follows since $a\in Z(A,+)$. Now we prove the second claim:

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

pro:socle

Proposition 4.36. *Let A be a brace. Then $\mathrm{Soc}(A)$ is an ideal of A.*

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

For each $d\in A$, $a+c'\circ d=c'\circ d+a$ by Lemma 4.35. Then

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

that is $\lambda_c(a)$ is central in $(A,+)$. Moreover,

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

and hence

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

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

As a corollary we obtain that the socle of a brace A is a trivial brace of abelian type. In particular, if $a\in\mathrm{Soc}(A)$, then a is a central element such that $a\circ b=a+b$ for all $b\in B$.

pro:soc_kernels

Proposition 4.37. *Let A be a brace. Then $\mathrm{Soc}(A)=\ker\lambda\cap\ker\mu$.*

Proof. Let $a \in \mathrm{Soc}(A)$. Then $\lambda_a = \mathrm{id}$ and $a \in Z(A,+)$. Let $c = \mu_a(b) = \lambda_b(a)' \circ b \circ a$. Then $b \circ a = \lambda_b(a) \circ c = (-b + b \circ a) \circ c$. Since this is equivalent to

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

it follows that $c' = b'$ and therefore $c = b$. 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 $a \in \mathrm{Soc}(A)$. □

Another important ideal was defined in [16].

Definition 4.38. Let A be a brace. The *annihilator* of A is defined as the set $\mathrm{Ann}(A) = \mathrm{Soc}(A) \cap Z(A,\circ)$.

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

Proposition 4.39. *The annihilator of a brace A is an ideal of A.*

Proof. Let $a \in A$ and $x \in \mathrm{Ann}(A)$. Since $\mathrm{Ann}(A) \subseteq Z(A,+) \cap Z(A,\circ)$, we only need to note that $\lambda_a(x) = x \in \mathrm{Ann}(A)$. □

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 4.40.** *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 4.41.** *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

$$\begin{aligned} a \circ x \circ a' &= a + \lambda_a(x \circ a') \\ &= a + \lambda_a(x + \lambda_x(a')) = a + \lambda_a(x) + \lambda_a\lambda_x(a') + a - a \\ &= a + \lambda_a(x + \lambda_x(a') - a') - a = a + \lambda_a(x + x * a') - a \end{aligned} \tag{4.11}$$

eq:trick:I*A

and hence I is an ideal.

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

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

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 brace homomorphism. The brace A/I is the *quotient brace* of A modulo I. It is possible to prove the isomorphism theorems for braces, see Exercises 4.14, 4.15, 4.16 and 4.17.

Exercises

prob:left_right **4.1.** Prove that there exists a bijective correspondence between left and right braces.

4.2. Let p be a prime number. Prove that $\mathbb{Z}/(p^2)$ is a brace of abelian type with the operation $x\circ y=x+y+pxy$.

4.3. Let A be a brace. Prove that

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

prob:star **4.4.** Let A be an additive (not necessarily abelian) group. Prove that a brace structure over A is equivalent to an operation $A\times A\to A$, $(a,b)\mapsto a*b$, such that

$$a*(b+c)=a*b+b+a*c-b$$

holds for all $a,b,c\in A$, and the operation $a\circ b=a+a*b+b$ turns A into a group.

prob:equivalences **4.5.** Let $(A,+,\circ)$ be a triple, where $(A,+)$ and $(A,\circ)$ are groups, and let $\lambda\colon A\to\mathbb{S}_A$, $a\mapsto\lambda_a$, $\lambda_a(b)=-a+a\circ b$. Prove that the following statements are equivalent:

1) A is a brace.
2) $\lambda_{a\circ b}(c)=\lambda_a\lambda_b(c)$ for all $a,b,c\in A$.
3) $\lambda_a(b+c)=\lambda_a(b)+\lambda_a(c)$ for all $a,b,c\in A$.

prob:2sided **4.6.** Let A be a brace such that $\lambda_a(a)=a$ for all $a\in A$. Then A is two-sided.

prob:Lau **4.7.** Prove Equality (4.7).

prob:radical **4.8.** Recall that two-sided braces are equivalent to radical rings. Prove that under this equivalence, (left) ideals of the radical ring correspond to (left) ideals of the associated brace.

prob:sum_ideals **4.9.** Prove that the intersection of ideals is an ideal.

4.10. Let A be a brace and I be a characteristic subgroup of the additive group of A. Prove that I is a left ideal of A.

4.11. Let $A = \dots$. Prove that A has only three ideals:... Let I be the ideal of A of size four. Prove that $A * I$ has size two and hence it is not an ideal of A.

prob:Bachiller1

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

prob:Bachiller2

4.13. Prove that the socle of a brace A is the kernel of the group homomorphism $(A,\circ) \to \mathrm{Aut}(A,+) \times \mathrm{Aut}(A,+)$, $a \mapsto (\lambda_a, \xi_a)$, where $\xi_a(b) = a + \lambda_a(b) - a$.

prob:iso1

4.14. Let $f \colon A \to B$ be a brace homomorphism. Prove that $A/\ker f \simeq f(A)$.

prob:iso2

4.15. Let A be a brace and B be a subbrace of A. If I is an ideal of B, then $B \circ I$ is a subbrace of B, $B \cap I$ is an ideal of B and $(B \circ I)/I \simeq B/(B \cap I)$.

prob:iso3

4.16. Let A be a brace and I and J be ideals of A. If $I \subseteq J$, then $A/J \simeq (A/I)/(J/I)$.

prob:correspondence

4.17. Let A be a brace and I be an ideal of A. There is a bijective correspondence between (left) ideals of A containing I and (left) ideals of A/I.

Notes

Braces of abelian type were introduced by Rump in [56] for studying involutive solutions to the YBE. Rump's definition was reformulated by Cedó, Jespers and Okniński in [21]. With this definition at hand, Guarnieri and Vendramin introduced arbitrary braces in [37].

Exercise 4.5 combines results of Bachiller, Rump [56] and Gateva–Ivanova [35]. Exercise 4.6 comes from [21].

Theorem 4.18 was proved by Rump in [56].

Theorem 4.20 was proved by Lau [46] and independently by Kinyon (unpublished). It answers a question of Cedó, Gateva–Ivanova and Smoktunowicz, see [19].

Theorem 4.22 was proved for braces of abelian type appears implicit in the work [56] of Rump, see also [21]. The general case was proved by Guarnieri and Vendramin in [37].

Theorem 4.24 was proved by Smoktunowicz and Vendramin in [63].

Exercise 4.6 comes from [21]. Exercises 4.12 and 4.13 appear in [8].

The socle was defined by Rump in [56]. The annihilator first appeared in the work [16] of Catino, Colazzo and Stefanell.

Chapter 5
Complements

cocycles

A

An **extension** of K by Q is a short exact sequence

$$1 \longrightarrow K \longrightarrow G \longrightarrow Q \longrightarrow 1$$

This means that G is a group with a normal subgroup N isomorphic to K such that $G/N \simeq Q$.

Example 5.1. C_6 and $\mathbb{S}_3$ are both extensions of C_3 by C_2.

Example 5.2. C_6 is an extension of C_2 by C_3.

Example 5.3. 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 5.4. 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 $E: \ 1 \longrightarrow K \longrightarrow G \longrightarrow Q \longrightarrow 1$ be an extension. A **lifting** of E is a map $\ell\colon Q \to G$ such that $p(\ell(x)) = x$ for all $x \in Q$.

xca:lifting **Exercise 5.5.** 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 $\ell(xy)\ker p = \ell(x)\ell(y)\ker p$.

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

Let Q and K be groups. Assume that Q acts by automorphism on K. A map $\varphi\colon Q \to K$ is said to be a **1-cocycle** (or a derivation) if

$$\varphi(xy) = \varphi(x)(x \cdot \varphi(y))$$

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 5.6. Let Q acts on K by automorphisms. For each $k \in K$, the map $Q \to K$, $x \mapsto [k,x] = kxk^{-1}x^{-1}$, is a derivation.

xca:1cocycle

Exercise 5.7. Let $\varphi\colon Q \to K$ be a 1-cocycle.

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

A subgroup K of 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 semidirect product $G = K \rtimes Q$, where K is a normal subgroup of G and Q is a subgroup of G such that $K \cap Q = \{1\}$.

thm:complements

Theorem 5.8. *Let Q acts by automorphism on K. Then there exists a bijective correspondence between the set $\mathscr{C}$ of complements K in $K \rtimes Q$ and the set* $\mathrm{Der}(Q,K)$ *of 1-cocycles $Q \to K$.*

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

We claim that $\delta_C \in \mathrm{Der}(Q,K)$. 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 $\delta(xx_1)xx_1 = cc_1 = \delta(x)x\delta(x_1)x_1$ implies that $\delta(xx_1) = \delta(x)x\delta(x_1)x^{-1}$. So there is a map $F\colon \mathscr{C} \to \mathrm{Der}(Q,K)$, $F(C) = \delta_C$.

We now construct a map $G\colon \mathrm{Der}(Q,K) \to \mathscr{C}$. For each $\delta \in \mathrm{Der}(Q,K)$ 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 $\delta(1) = 1$, $1 \in X$. 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

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

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 $G\colon \mathrm{Der}(Q,K) \to \mathscr{C}$, $G(\delta) = \Delta$.

We claim that $G \circ F = \mathrm{id}_{\mathscr{C}}$. Let $C \in \mathscr{C}$. 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 $F \circ G = \mathrm{id}_{\mathrm{Der}(Q,K)}$. Let $\delta \in \mathrm{Der}(Q,K)$. 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 $\delta(x) = \delta(y)$ by the uniqueness. □

Let the group Q acts by automorphism on K. A derivation $\delta \in \mathrm{Der}(Q,K)$ 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

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

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

theorem:Sysak

Theorem 5.9 (Sysak). *Sean Q y K grupos tales que Q actúa por automorfismos en K. Sea $\delta \in \mathrm{Der}(Q,K)$.*

1) *$\Delta = \{\delta(x)x : x \in Q\}$ es un complemento para K en $K \rtimes Q$.*
2) *$\delta \in \mathrm{Inn}(Q,K)$ si y sólo si Q y Δ son conjugados en K.*
3) *$\ker\delta = Q \cap \Delta$.*
4) *δ es sobreyectiva si y sólo si $K \rtimes Q = \Delta Q$.*

Proof. In the proof of Theorem 5.8 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

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

Moreover, $\Delta Q \subseteq K \rtimes Q$, as $\delta(x) \in K$ for all $x \in Q$. Conversely, if $k \in K$ y $x \in Q$ there exist $y,z \in Q$ such that $kx = \delta(y)yz$. Then it follows that $k = \delta(y)$. □

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

Corollary 5.10. *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.*

Another consequence:

xca:ker1cocycle

Exercise 5.11. 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 $Q \cap \Delta = \{1\}$.

B

lem:1cocycle

Lemma 5.12. *Let G be a group and N be a normal subgroup of G. If G acts on N by conjugation and $\varphi\colon G \to N$ is a 1-cocycle with kernel K, then $\varphi(x) = \varphi(y)$ if and only if $xK = yK$. In particular, $(G:K) = |\varphi(G)|$.*

Proof. If $\varphi(x) = \varphi(y)$, then, since

$$\varphi(x^{-1}y) = \varphi(x^{-1})(x^{-1}\cdot\varphi(y)) = \varphi(x^{-1})(x^{-1}\cdot\varphi(x)) = \varphi(x^{-1}x) = \varphi(1) = 1,$$

we obtain that $xK = yK$. Conversely, if $x^{-1}y \in K$, then, since

$$1 = \varphi(x^{-1}y) = \varphi(x^{-1})(x^{-1}\cdot\varphi(y)),$$

we conclude that $\varphi(y) = x\cdot\varphi(x^{-1})^{-1}$. Thus $\varphi(x) = \varphi(y)$.

The second claim is now trivial, as φ is constant in each coset of K and there are $(G:K)$ different possible values. □

lem:d

Lemma 5.13. *Let G be a finite group, N be a normal abelian subgroup of G and S, T and U be transversal ofN in G. Let*

$$d(S,T) = \prod st^{-1} \in N,$$

where the product is taken over all $s \in S$ and $t \in T$ such that $sN = tN$. The following statements hold:

1) *$d(S,T)d(T,U) = d(S,U)$.*
2) *$d(gS,gT) = gd(S,T)g^{-1}$ for all $g \in G$.*
3) *$d(nS,S) = n^{(G:N)}$ for all $n \in N$.*

Proof. If $s \in S$, $t \in T$ and $u \in U$ are such that $sN = tN = uN$, then, since N is abelian and $(st^{-1})(tu^{-1}) = su^{-1}$,

$$d(S,T)d(T,U) = \prod(st^{-1})(tu^{-1}) = \prod su^{-1} = d(S,U).$$

Since $sN = tN$ if and only if $gsN = gtN$ for all $g \in G$,

$$g\left(\prod st^{-1}\right)g^{-1}=\prod gst^{-1}g^{-1}=\prod(gs)(gt)^{-1}=d(gS,gT).$$

Finally, since N is normal, $nsN=sN$ for all $n\in N$. Thus

$$d(nS,S)=\prod(ns)s^{-1}=n^{(G:N)}.$$ □

We now prove the first version of Schur–Zassenhaus' theorem.

:SchurZassenhaus:abelian

Theorem 5.14 (Schur–Zassenhaus). *Let G be a finite group and N be an abelian normal subgroup of G. If $|N|$ and $(G:N)$ are coprime, then N admits a complement in G. In this case, all complements of N are conjugate in G.*

Proof. Let T be a transversal of N in G. Let $\theta\colon G\to N$, $\theta(g)=d(gT,T)$. Since N is abelian, Lemma 5.13 implies that θ is a 1-cocycle, where G acts on N by conjugation:

$$\begin{aligned}\theta(xy)&=d(xyT,T)=d(xyT,xT)d(xT,T)\\&=(xd(yT,T)x^{-1})d(xT,T)=(x\cdot\theta(y))\theta(x).\end{aligned}$$

Claim. $\theta|_N\colon N\to N$ is surjective.

If $n\in N$, then $\theta(n)=d(nT,T)=n^{(G:N)}$ by Lemma 5.13. Since $|N|$ and $(G:N)$ are coprime, there exist $r,s\in\mathbb{Z}$ such that $r|N|+s(G:N)=1$. Thus

$$n=n^{r|N|+s(G:N)}=(n^s)^{(G:N)}=\theta(n^s).$$

Let $H=\ker\theta$. We claim that H is a complement for N. We know that H is a subgroup of G. Since

$$|N|=|\theta(G)|=(G:H)=\frac{|G|}{|H|}$$

by Lemma 5.12, it follows that $N\cap H=\{1\}$ because $|N|$ and $(G:N)=|H|$ are coprime. Since $|NH|=|N||H|=|G|$, we conclude that $G=NH$ and hence H is a complement of N in G.

We now prove that two complements of N in G are conjugate. Let K be a complement of N in G. Since $NK=G$ and $N\cap K=\{1\}$, it follows that K is a transversal of N in G. Let $m=d(T,K)\in N$. Since $\theta|_N$ is surjective, there exists $n\in N$ such that $\theta(n)=m$. By Lemma 5.13, for each $k\in K$,

$$kmk^{-1}=kd(T,K)k^{-1}=d(kT,kK)=d(kT,K)=d(kT,T)d(T,K)=\theta(k)m$$

holds. Since N is abelian, $\theta(n^{-1})=m^{-1}$ and hence

$$\begin{aligned}\theta(nkn^{-1})&=\theta(n)n\theta(kn^{-1})n^{-1}=m\theta(kn^{-1})\\&=m\theta(k)k\theta(n^{-1})k^{-1}=m\theta(k)km^{-1}k^{-1}=1.\end{aligned}$$

Therefore $nKn^{-1}\subseteq H=\ker\theta$. Since $|K|=(G:N)=|H|$, we conclude that $nKn^{-1}=H$. □

The general version of Schur–Zassenhaus' theorem does not need N to be abelian.

thm:SchurZassenhaus

Theorem 5.15 (Schur–Zassenhaus). *Let G be a finite group and N be a normal subgroup of G. If $|N|$ and $(G:N)$ are coprime, then N admits a complement in G.*

Proof. We proceed by induction on $|G|$. If there exists a proper subgroup K of G such that $NK=G$, then, since $(K:K\cap N)=(G:N)$ is coprime with $|N|$, it coprime with $|K\cap N|$. Moreover, $K\cap N$ is normal in K. By inductive hypothesis, $K\cap N$ admits a complement in K. Hence there exists a subgroup H of K such that

$$|H|=(K:K\cap N)=(G:N).$$

Supongamos entonces que no existe un subgrupo propio K de G tal que $NK=G$. Podemos suponer que $N\neq 1$ (de lo contrario, basta tomar G como complemento de N en G). Como N está contenido en todo subgrupo maximal de G (pues si existe un maximal $M\subsetneq G$ tal que $N\not\subseteq M$ entonces $NM=G$), se tiene que $N\subseteq\Phi(G)$. Por el teorema de Frattini 6.54, $\Phi(G)$ es nilpotente y luego N es nilpotente; en particular, $Z(N)\neq\{1\}$. Sea $\pi\colon G\to G/Z(N)$ el morfismo canónico. Como N es normal en G y $Z(N)$ es característico en N, $Z(N)$ es normal en G. Además

$$(\pi(G):\pi(N))=\frac{|\pi(G)|}{|\pi(N)|}=\frac{|G/Z(N)|}{|N/N\cap Z(N)|}=(G:N)$$

es coprimo con $|N|$, y entonces es también coprimo con $|\pi(N)|$. Por hipótesis inductiva, $\pi(N)$ admite un complemento en $G/Z(N)$, digamos $\pi(K)$ para algún subgrupo K de G. Luego $G=NK$ pues $\pi(G)=\pi(N)\pi(K)=\pi(NK)$. Como entonces $K=G$ (pues sabíamos que no existe K tal que $G=NK$), $\pi(N)$ es abeliano pues

$$\pi(Z(N))=\pi(N)\cap\pi(K)=\pi(N)\cap\pi(G)=\pi(N).$$

Luego $N\subseteq Z(N)$ es abeliano y entonces, por el teorema **??**, el subgrupo N admite un complemento. □

urZassenhaus:conjugacion

Theorem 5.16. *Let G be a fintie group and N be a normal subgroup of G such that $|N|$ and $(G:N)$ are coprime. If either N or G/N is solvable, then all complements of N in G are conjugate.*

Proof. Let G be a minimal counterexample, so there are complements K_1 and K_2 of N in G such that K_1 and K_2 are not conjugate and $|G|$ is minimal with this property.

Claim. Each subgroup U of G satiasfies the hypotheses of the theorem with respect to the normal subgroup $U\cap N$.

Since N is normal in G, the subgroup $U\cap N$ is normal in U. Moreover, $|U\cap N|$ and $(U:U\cap N)$ are coprime, as $|U\cap N|$ divides $|N|$ and $(U:U\cap N)=(UN:N)$ divides $(G:N)$. If G/N is solvable, then $U/U\cap N$ is solvable since $U/U\cap N$ is isomorphic to a subgroup of G/N. If N is solvable, the subgroup $U\cap N$ is solvable.

Claim. If thre is a normal subgroup L of G such that $\pi(N)$ is normal in $\pi(G)$, where $\pi\colon G\to G/L$ is the canonical map, then $\pi(G)$ satifies the hypotheses of the theorem with respect to $\pi(N)$. In this case, if H is a complement of N in G, then $\pi(H)$ is a complement of $\pi(N)$ in $\pi(G)$.

If N is solvable, then $\pi(N)$ is solvable. If G/N is solvable, then the group $\pi(G)/\pi(N)\simeq G/NL$ is solvable. Moreover, $(\pi(G):\pi(N))=\frac{|G/L|}{|N/N\cap L|}$ divides the index $(G:N)$ of N in G.

If H is a complement of N in G, $|\pi(H)|$ and $|\pi(N)|$ are coprime. Thus $\pi(H)$ is a complement of $\pi(N)$, as $\pi(G)=\pi(N)\pi(H)=\pi(NH)$ and $\pi(N)\cap\pi(H)=\{1\}$.

Claim. N is minimal normal in G.

Let $M\neq\{1\}$ be a normal subgroup of G such that $M\subseteq N$. Let $\pi\colon G\to G/M$ be the canonical map. The group $\pi(G)$ satiafies the hypotheses of the theorem with respect to the normal subgroup $\pi(N)$. By the minimality of $|G|$, there exists $x\in G$ such that $\pi(xK_1x^{-1})=\pi(K_2)$. The subgroup $U=MK_2$ satisfies the hypotheses of the theorem with respect to the normal subgroup $U\cap N$. Since $xK_1x^{-1}\cup K_2\subseteq U$, we conclude that xK_1x^{-1} and K_2 are complements of $U\cap N$ in U. Thus $MK_2=G$, as xK_1x^{-1} and K_2 are not conjugate and $|G|$ is minimal. Therefore $M=N$, as

$$\frac{|K_2|}{|M\cap K_2|}=(MK_2:M)=(G:M)=\frac{|NK_2|}{|M|}=(N:M)|K_2|.$$

Claim. N is not solvable and G/N is solvable.

Otherwise, by Lemma **??**, N is minimal normal and hence abelian. This yields a contradiction, as the previous version of the Schur–Zassenhaus's theorem implies that K_1 and K_2 are conjugate.

Let $p\colon G\to G/N$ be the canonical map and S be such that $p(S)$ is minimal normal in $p(G)=G/N$. By Lemma **??**, $p(S)$ is a p-group for some prime number p. Since $G=NK_1=NK_2$ and $N\subseteq S$, Dedekind's lemma implies that

$$S=N(S\cap K_1)=N(S\cap K_2).$$

Thus $S\cap K_1$ and $S\cap K_2$ are complements of N in S. Since

$$p(S)=p(S\cap K_1)=p(S\cap K_2)$$

is a p-group, p divides $|S|$. The group S satisafies the hypotheses of the theorem with respect to the normal subgroup N, so $|N|$ and $(S:N)$ are coprime. If $p\mid |N|$, then $p\nmid (S:N)=|p(S)|$, a contradiction. Therefore $p\nmid |N|$. This implies that $S\cap K_1$ and $S\cap K_2$ are Sylow p-subgroups of S, as

$$|S\cap K_1|=(S:N)=|S\cap K_2|.$$

By the second Sylow's theorem, there exists $s\in S$ such that

$$S \cap sK_1s^{-1} = S \cap K_2.$$

In particular, $S \neq G$ by the minimality of $|G|$. Let

$$L = S \cap K_2 = S \cap sK_1s^{-1} \neq \{1\}.$$

Since S is normal in G, it follows that $sK_1s^{-1} \cup K_2 \subseteq N_G(L)$ (because L is normal both in sK_1s^{-1} and in K_2). The subgroups $sK_1s^{-1} \subseteq N_G(L)$ and $K_2 \subseteq N_G(L)$ are complements of $N \cap N_G(L)$ in $N_G(L)$. Thus $N_G(L) = G$ by the minimality of $|G|$ (if $N_G(L) \neq G$, then both sK_1s^{-1} and K_2 are conjugate in G because they are conjugate in $N_G(L)$). Therefore L is normal in G.

Let $\pi_L \colon G \to G/L$ be the canonical map. Since both $\pi_L(K_1)$ and $\pi_L(K_2)$ are complements of $\pi_L(N)$ in $\pi_L(G)$, the minimality of $|G|$ implies that there exists $g \in G$ such that $\pi_L(gK_1g^{-1}) = \pi_L(K_2)$, so there exists $g \in G$ such that $(gK_1g^{-1})L = K_2L$. Thus $gK_1g^{-1} \cup K_2 \subseteq \langle K_2, L\rangle = K_2$, as $L \subseteq K_2$. In conclusion, $gK_1g^{-1} = K_2$, a contradiction to the minimality of $|G|$. □

By Feit–Thompson´s theorem, we do not need to assume that N or G/N is solvable. Indeed, since every group of odd order is solvable and $|N|$ and $(G:N)$ are coprime, it follows that either $|N|$ or $(G:N)$ is odd.

C

Let G be a finite group and π be a set of (positive) prime numbers. We say that G is a π-group if all prime divisors of $|G|$ belong to π. A π-subgroup of G is a subgroup of G that is also a π-group. A π-number is an integer with all prime divisors in π. The complement of π is the set of prime numbers will be denoted by π'. A π'-number is then an integer not divisible by the primes of π.

Let π be a set of primes.A subgroup H of a group G is a **Hall π-subgroup** if H is a π-subgroup of G and the index $(G:H)$ is a π'-number.

thm:HallE

Theorem 5.17 (Hall). *Let π be a set of primes and G be a finite solvable group. Then G admits a Hall π-subgroup.*

Proof. Assume that $|G| = nm > 1$ with $\gcd(n,m) = 1$. We prove by induction on $|G|$ that there exists a subgroup of order m. Let K be a minimal normal subgroup of G and let $\pi \colon G \to G/K$ be the canonical map. (We are using π for a fixed set of primes and for the canonical map $G \to G/K$, but hopefully no confusion will arise.) Since G is solvable, K is an abelian p-group by Lemma **??**.

There are two cases to consider. Assume first that p divides m. Since $|G/K| < |G|$, the inductive hypothesis and the correspondence theorem imply that there exists a subgroup J of G containing K such that $\pi(J)$ is a subgroup of $\pi(G) = G/K$ of order $m/|K|$. Thus $|J| = m$ since

$$m/|K| = |\pi(J)| = \frac{|J|}{|K \cap J|} = (J : K).$$

Assume now tht p does not divide m. The inductive hypothesis and the correspondence theorem imply that there exists a subgroup H of G containing K such that $\pi(H)$ is a subgroup of G/K of order m. Since $|H| = m|K|$, K is normal in H and $|K|$ is coprime with $|H : K|$, Schur–Zassenhaus's theorem (Theorem 5.14) implies that there exists a complement J of K in H. Thus J is a subgroup of G of order $|J| = m$. □

Example 5.18. The group $\mathbb{A}_5$ contains a Hall $\{2,3\}$-subgroup isomorphic to $\mathbb{A}_4$.

Example 5.19. The simple group $\mathbf{PSL}_3(2)$ of order 168 does not contain Hall $\{2,7\}$-subgroups.

thm:HallC

Theorem 5.20 (Hall). *Let G be a finite solvable group and π be a set of primes. All Hall π-subgroups of G are conjugate.*

Proof. Podemos suponer que $G \neq \{1\}$. Procederemos por inducción en $|G|$. Sean H y K dos π-subgrupos de Hall de G. Sea M un subgrupo de G minimal-normal y sea $\pi\colon G \to G/M$ el morfismo canónico. Como G es resoluble, el lema **??** implica que M es un p-grupo para algún primo p. Como $\pi(H)$ y $\pi(K)$ son π-subgrupos de Hall de G/M, los subgrupos $\pi(H)$ y $\pi(K)$ con conjugados en G/M. Luego existe $g \in G$ tal que $gHMg^{-1} = KM$.

Hay dos casos a considerar. Supongamos primero que $p \in \pi$. Como $|HM|$ y $|KM|$ son π-números y $|H| = |K|$ es el mayor π-número que divide al orden de G, se concluye que $H = HM$ y $K = KM$. En particular, $gHg^{-1} = K$.

Supongamos ahora que $p \notin \pi$. Es evidente que K complementa a M en KM pues $K \cap M = 1$. Veamos que gHg^{-1} complementa a M en KM: como M es normal en G,

$$(gHg^{-1})M = gHMg^{-1} = KM,$$

y $gHg^{-1} \cap M = 1$ ya que $p \notin \pi$. Estos complementos tienen que ser conjugados por el teorema de Schur–Zassenhaus **??**. □

Corollary 5.21. *Sea G un grupo finito y sea N un subgrupo normal de G de orden n. Supongamos que N o G/N es resoluble. Si $|G : N| = m$ es coprimo con n y m_1 divide a m, todo subgrupo de G de orden m_1 está contenido en algún subgrupo de orden m.*

Proof. Sea H un complemento para N en G. Entonces $|H| = m$. Sea H_1 subgrupo de G tal que $|H_1| = m_1$. Como n y m son coprimos, $m_1 = |H_1| = |H \cap NH_1|$ pues

$$\frac{|H||N||H_1|}{|H \cap NH_1|} = \frac{|H||NH_1|}{|H \cap NH_1|} = |H(NH_1)| = |G| = |NH| = |N||H|.$$

Como H_1 y $H \cap NH_1$ son complementos para N en NH_1, ambos de orden coprimo con n, existe $g \in G$ tal que $H_1 = g(H \cap NH_1)g^{-1}$. Luego $H_1 \subseteq gHg^{-1}$ y entonces $|gHg^{-1}| = m$. □

D

Let A be an additive group and G be a group and let $G\times A\to A$, $(g,a)\mapsto g\cdot a$, is 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-*cocycle* is a bijective map $\pi\colon G\to A$ such that

$$\pi(gh)=\pi(g)+g\cdot\pi(h) \tag{5.1}$$ eq:1cocycle

for all $g,h\in G$. We now prove the equivalence between braces and bijective 1-cocycles.

thm:1cocycle **Theorem 5.22.** *Over any additive group A the following data are equivalent:*

1) *A group G and a bijective 1-cocycle $\pi\colon G\to A$.*
2) *A brace structure over 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 Proposition 4.12, $a\mapsto\lambda_a$, is a group homomorphism and hence G acts on A by automorphisms. Then (5.1) holds and therefore $\pi\colon G\to A$ is a bijective 1-cocycle. □

The construction of Theorem 5.22 is functorial, see Exercise 5.1.

exa:d8q8 **Example 5.23.** 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

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

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.

Exercises

prob:1cocycle

5.1. Let $\pi\colon G\to A$ and $\eta: H\to B$ 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

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

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.

Open problems

Notes

In the case of braces of abelian type, Theorem 5.22 is implicit in the work of Rump, see [56, 57] or [21]. Similar results appear in the work of Etingof, Schedler and Soloviev [32], Lu, Yan and Zhu [48] and Soloviev [64]. In [31] Etingof and Gelaki give a method of constructing finite-dimensional complex semisimple triangular Hopf algebras. They show how any non-abelian group which admits a bijective 1-cocycle gives rise to a semisimple minimal triangular Hopf algebra which is not a group algebra.

Chapter 6
Nilpotent groups

nilpotent

A

If G is a group and $x, y, z \in G$, the conjugation (as a left action) will be denoted by ${}^{x}y = xyx^{-1}$. The commutator between x and y is then

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

We also write $[x,y,z] = [x,[y,z]]$. If X, Y and Z are subgroups of G, we write

$$[X,Y] = \langle [x,y] : x \in X,\, y \in Y \rangle$$

and $[X,Y,Z] = [X,[Y,Z]]$. Since $[X,Y] = [Y,X]$, it follows that $[X,Y,Z] = [X,Z,Y]$.

xca:HallWitt **Exercise 6.1 (Hall–Witt).** Let G be a group and $x, y, z \in G$. Then

$$\left({}^{y}[x,y^{-1},z]\right)\left({}^{z}[y,z^{-1},x]\right)\left({}^{x}[z,x^{-1},y]\right) = 1. \tag{6.1}$$ eq:HallWitt

Note that if G is such that $[G,G]$ is central, then Hall–Witt's identity turns out to be Jacobi's identity.

lemma:3subgrupos_general **Lemma 6.2 (three subgroups lemma).** *Let N be a normal subgroup of G and let X, Y and Z be subgroups of G. If $[X,Y,Z] \subseteq N$ and $[Y,Z,X] \subseteq N$, then $[Z,X,Y] \subseteq N$.*

Proof. We first prove the lemma in the case where $N = \{1\}$. Since $[x,y] \in C_G(z)$ implies that $[X,Y] \subseteq C_G(Z)$, it is enough to prove that $[z,x^{-1},y] = 1$ for all $x \in X$, $y \in Y$ and $z \in Z$, Since $[y^{-1},z] \in [Y,Z]$, it follows that $[x,y^{-1},z] \in [X,Y,Z] = \{1\}$. Thus ${}^{y}[x,y^{-1},z] = 1$. Similarly, ${}^{z}[y,z^{-1},x] = 1$. Hence the Hall–Witt identity yields $[z,x^{-1},y] = 1$.

We now demonstrate the general case. Let N be a normal subgroup of G and $\pi\colon G \to G/N$ be the canonical map. Since $[X,Y,Z] \subseteq N$,

$$\begin{aligned}\{1\} &= \pi([X,Y,Z]) = \pi([X,[Y,Z]]) \\ &= [\pi(X),\pi([Y,Z])] = [\pi(X),[\pi(Y),\pi(Z)]] = [\pi(X),\pi(Y),\pi(Z)].\end{aligned}$$

Similarly one proves that $[\pi(Y),\pi(Z),\pi(X)] = \{1\}$. By the previous paragraph, $[\pi(Z),\pi(X),\pi(Y)] = \{1\}$, so $[Z,X,Y] \subseteq N$. $\square$

The **lower central series** of a group G is the sequence $\gamma_k(G)$, $k \in \mathbb{N}$, defined recursively as

$$\gamma_1(G) = G, \quad \gamma_{i+1}(G) = [G,\gamma_i(G)] \quad i \geq 1.$$

A group G is said to be **nilpotent** if there exists positive integer c such that $\gamma_{c+1}(G) = \{1\}$. The smallest c such that $\gamma_{c+1}(G) = \{1\}$ is the **nilpotency index** (or **nilpotency class**) of G.

Example 6.3. A group is nilpotent of class one if and only if it is abelian.

Example 6.4. The group $G = \mathbb{A}_4$ is not nilpotent, as

$$\gamma_1(G) = G, \quad \gamma_j(G) = \{\mathrm{id},(12)(34),(13)(24),(14)(23)\} \simeq C_2 \times C_2$$

for all $j \geq 2$.

xca:gamma

Exercise 6.5. Let G be group. Prove the following statements:

1) Each $\gamma_i(G)$ is a characteristic group of G.
2) $\gamma_i(G) \supseteq \gamma_{i+1}(G)$ for all $i \geq 1$.
3) If $f\colon G \to H$ is a surjective group homomorphism, then $f(\gamma_i(G)) = \gamma_i(H)$ for all $i \geq 1$.

theorem:nilpotent

Theorem 6.6. *Let G be a nilpotent group.*

1) *If H is a subgroup of G, then H is nilpotent.*
2) *If $f\colon G \to H$ is a surjective group homomorphism, then H is nilpotent.*

Proof. For the first statement note that $\gamma_i(H) \subseteq \gamma_i(G)$ for all $i \geq 1$. Let us prove the second claim, if there exists c such that $\gamma_{c+1}(G) = \{1\}$, then

$$\gamma_{c+1}(H) = f(\gamma_{c+1}(G)) = f(\{1\}) = \{1\}. \qquad \square$$

Example 6.7. The group $\mathbf{SL}_2(3)$ is not nilpotent, as $\mathbb{A}_4$ is a quotient of $\mathbf{SL}_2(3)$.

There exist a non-nilpotent group G with a normal subgroup K such that K and G/K are both nilpotent. For example, take $G = \mathbb{S}_3$ and $K = \mathbb{A}_3$.

Exercise 6.8. Let p be a prime number. Prove that finite p-groups are nilpotent.

theorem:gamma

Theorem 6.9. *Let G be a group. Then $[\gamma_i(G),\gamma_j(G)] \subseteq \gamma_{i+j}(G)$ for all $i, j \geq 1$.*

Proof. We proceed by induction on i. The case where $i = 1$ is trivial, as by definition one has $[G,\gamma_j(G)] = \gamma_{j+1}(G)$. Assume now that the result holds for some $i \geq 1$ and all $j \geq 1$. We first note that

$$[G,\gamma_i(G),\gamma_j(G)] = [G,\gamma_{i+j}(G)] \subseteq \gamma_{i+j+1}(G)$$

by the inductive hypothesis. Moreover, again using the inductive hypothesis,

$$[\gamma_i(G),\gamma_j(G),G]=[\gamma_i(G),G,\gamma_j(G)]=[\gamma_i(G),\gamma_{j+1}(G)]\subseteq\gamma_{i+j+1}(G).$$

Lemma 6.2 implies that $[\gamma_j(G),G,\gamma_i(G)]\subseteq\gamma_{i+j+1}(G)$. Thus

$$[\gamma_{i+1}(G),\gamma_j(G)]=[[G,\gamma_i(G)],\gamma_j(G)]=[\gamma_j(G),G,\gamma_i(G)]\subseteq\gamma_{i+j+1}(G). \qquad \square$$

Certainly we can consider other type of arbitrary commutators, say for example $[[G,G],G]$ and $[G,G,G]=[G,[G,G]]$. This naturally suggest the notion of the weight of a commutator. For example, $[[G,G],G]$ and $[G,G,G]=[G,[G,G]]$ are both commutators of weight three.

Corollary 6.10. *Every commutator of weight n is contained in $\gamma_n(G)$.*

Proof. We proceed by induction on n. The case $n=1$ is trivial, so assume that the result holds for some $n\geq 1$. Let $[A,B]$ be a commutator, where A is a commutator of weight k, B is a commutator of weight l and $n+1=k+l$. Since $k<n$ and $l<n$, the inductive hypothesis implies that $A\subseteq\gamma_k(G)$ y $B\subseteq\gamma_l(G)$. Thus

$$[A,B]\subseteq[\gamma_k(G),\gamma_l(G)]\subseteq\gamma_{k+l}(G)$$

by the previous theorem. $\square$

Nilpotent groups satisfy the normalizer condition. A group G satisfies the **normalizer condition** if each proper subset is smaller than its normalizer.

lem:normalizer

Lemma 6.11 (normalizer condition). *Let G be a nilpotent group. If H is a proper subgroup of G, then $H\subsetneq N_G(H)$.*

Proof. Since G is nilpotent, there a positive integer c such that

$$G=\gamma_1(G)\supseteq\cdots\supseteq\gamma_{c+1}(G)=\{1\}.$$

Since $\{1\}=\gamma_{c+1}(G)\subseteq H$ and $\gamma_1(G)\not\subseteq H$, let k be the smallest positive integer such that $\gamma_k(G)\subseteq H$. Since

$$[H,\gamma_{k-1}(G)]\subseteq[G,\gamma_{k-1}(G)]=\gamma_k(G)\subseteq H,$$

it follows that $xHx^{-1}\subseteq H$ for all $x\in\gamma_{k-1}(G)$, so $\gamma_{k-1}(G)\subseteq N_G(H)$. If $N_G(H)=H$, then $\gamma_{k-1}(G)\subseteq H$, a contradiction to the minimality of k. $\square$

For a group G we define the sequence $\zeta_0(G),\zeta_1(G),\dots$ recursively as

$$\zeta_0(G)=\{1\},\quad \zeta_{i+1}(G)=\{g\in G:[x,g]\in\zeta_i(G)\text{ para todo }x\in G\},\quad i\geq 0.$$

In particular, $\zeta_1(G)=Z(G)$.

lem:central_ascendente

Lemma 6.12. *Let G be a group. Each $\zeta_i(G)$ is a normal subgroup of G.*

Proof. We proceed by induction on i. The case $i = 0$ is trivial, as $\zeta_0(G) = \{1\}$. Assume that the result holds for some $i \geq 0$. We claim that $\zeta_{i+1}(G)$ is a subgroup of G. Let $g,h \in \zeta_{i+1}(G)$ and $x \in G$. The inductive hypothesis implies that

$$[g^{-1},x] = (xg^{-1})[g,x^{-1}](xg^{-1})^{-1} \in (xg^{-1})\zeta_i(G)(xg^{-1})^{-1} = \zeta_i(G),$$
$$[gh,x] = [g,hxh^{-1}][h,x] \in \zeta_i(G).$$

Since $1 \in \zeta_{i+1}(G)$, the sets $\zeta_i(G)$ are subgroups of G.

To prove that each subgroup is normal we also proceed by induction on i. If $g \in \zeta_{i+1}(G)$ and $x \in G$, then $xgx^{-1} \in \zeta_{i+1}(G)$. Indeed,

$$[xgx^{-1},y] = x[g,x^{-1}yx]x^{-1} \in \zeta_i(G)$$

for all $y \in G$. □

For a group G the **ascending central series** of G is the sequence

$$\{1\} = \zeta_0(G) \subseteq \zeta_1(G) \subseteq \zeta_2(G) \subseteq \cdots$$

A group G is said to be **perfect** if $[G,G] = G$. Note that G is perfect if and only if $G/[G,G]$ is trivial. The alternating simple group $\mathbb{A}_5$ is the smallest non-trivial perfect group.

Example 6.13. The groups $\mathbf{SL}_2(2)$ and $\mathbf{SL}_2(3)$ are not perfect.

Let p be a prime number and $q = p^m$ for some $m \in \mathbb{N}$. The groups $\mathbf{SL}_n(q)$ are perfect except the cases $\mathbf{SL}_2(2)$ and $\mathbf{SL}_2(3)$. As an example, let us prove that $\mathbf{SL}_2(q)$ is perfect if $p \geq 5$ is a prime number. We first claim that $\mathbf{SL}_2(q)$ is generated by matrices $X_{ij}(\lambda) = I + \lambda E_{ij}$, where I denotes the identity matrix, E_{ij} is the matriz with a one at position (i,j) and zero in all other entries, $i,j \in \{1,2\}$ and $\lambda \in \mathbb{F}_q \setminus \{0\}$. First note that a matrix $\begin{pmatrix} 1 & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(q)$ is a product of some of the $X_{ij}(\lambda)$, as

$$\begin{pmatrix} 1 & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ c & 1 \end{pmatrix} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} = X_{21}(c)X_{12}(b).$$

This implies that a matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(q)$ with $c \neq 0$ is also a product of some $X_{ij}(\lambda)$. Indeed, if λ is such that $a = 1 - \lambda c$, then

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & -\lambda \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & b+\lambda d \\ c & d \end{pmatrix} = X_{12}(-\lambda)X_{21}(c)X_{12}(b+\lambda d).$$

Finally,

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ a & b+d \end{pmatrix}$$

and therefore $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ is a product of some $X_{ij}(\lambda)$ since $\begin{pmatrix} a & b \\ a & b+d \end{pmatrix}$ is a product of some $X_{ij}(\lambda)$. To prove that $[\mathbf{SL}_2(q), \mathbf{SL}_2(q)] = \mathbf{SL}_2(q)$ we first note that

$$\left[\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}, \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \right] = \begin{pmatrix} 1 & (a^2-1)b \\ 0 & 1 \end{pmatrix}.$$

Since $q \geq 3$, given $\lambda \in \mathbb{F}_q$ and $a \in \mathbb{F}_q \setminus \{-1,0,1\}$, there exists $b \in \mathbb{F}_q$ such that $\lambda = (a^2-1)b$. This implies that each $X_{ij}(\lambda)$ belongs to the commutator subgroup of $\mathbf{SL}_2(q)$.

Exercise 6.14. Let $q \geq 5$. Prove that $\mathbf{SL}_n(q)$ is perfect.

Exercise 6.15. Let G be a perfect group and N be a normal subgroup of G. Then G/N is perfect.

theorem:Grun **Theorem 6.16 (Grün).** *If G is a perfect group, then $Z(G/Z(G)) = \{1\}$.*

Proof. The three subgroups lemma with $X = Y = G$, $Z = \zeta_2(G)$ and $N = \{1\}$ yields

$$\{1\} = [\zeta_2(G), G, G] = [\zeta_2(G), [G,G]] = [\zeta_2(G), G].$$

Thus $\zeta_2(G) \subseteq Z(G)$. Now we prove that $Z(G/Z(G))$ is trivial. Let $\pi\colon G \to G/Z(G)$ be the canonical map and $x \in G$ be such that $\pi(x)$ is a central element. Then

$$[\pi(x), \pi(y)] = \pi([x,y]) = 1$$

for all $y \in G$. In particular, $[x,y] \in Z(G) = \zeta_1(G)$ for all $y \in G$. This means that $x \in \zeta_2(G) \subseteq Z(G)$. $\square$

A subgroup K of G **normalizes** a subgroup H if $K \subseteq N_G(H)$. A subgroup K of G **centralizes** a subgroup H if $K \subseteq C_G(H)$, that is if and only if $[H,K] = \{1\}$.

lem:gamma_zeta **Lemma 6.17.** *Let G be a group. There exists c such that $\zeta_c(G) = G$ if and only if $\gamma_{c+1}(G) = \{1\}$. In this case,*

$$\gamma_{i+1}(G) \subseteq \zeta_{c-i}(G)$$

for all $i \in \{0,1,\dots,c\}$.

Proof. Assume first that $\zeta_c(G) = G$. To prove that $\gamma_{i+1}(G) \subseteq \zeta_{c-i}(G)$ we proceed by induction. The case where $i = 0$ is trivial, so assume the result holds for some $i \geq 0$. If $g \in \gamma_{i+2}(G) = [G, \gamma_{i+1}(G)]$, then

$$g = \prod_{k=1}^{N} [x_k, g_k],$$

for some $g_1, \dots, g_N \in \gamma_{i+1}(G)$ and $x_1, \dots, x_N \in G$. By the inductice hypothesis,

$$g_k \in \gamma_i(G) \subseteq \zeta_{c-i}(G)$$

for all k and thus $[x_k, g_k] \in \zeta_{c-i-1}(G)$ for all k. Hence $g \in \zeta_{c-(i+1)}(G)$. From this the claim follows.

Assume now that $\gamma_{c+1}(G) = \{1\}$. We prove that $\gamma_{i+1}(G) \subseteq \zeta_{c-i}(G)$ for all i. We proceed by backward induction on i. The case $i = c$ is trivial, so assume the result holds for some $i+1 \leq c$. Let $g \in \gamma_i(G)$. By the inductive hypothesis,

$$[x, g] \in [G, \gamma_i(G)] = \gamma_{i+1}(G) \subseteq \zeta_{c-i}(G).$$

Thus $g \in \zeta_{c-i+1}(G)$ by definition. □

Example 6.18. If $G = \mathbb{S}_3$, then $\zeta_j(G) = \{1\}$ for all $j \geq 0$:

A **central series** of a group G is a sequence

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

of normal subgroups of G such that for each $i \in \{1, \ldots, n\}$, $\pi_i(G_{i-1})$ is a subgroup of $Z(G/G_i)$, where $\pi_i \colon G \to G/G_i$ is the canonical map.

pro:serie_central

Proposition 6.19. *Let G be a group and $G = G_0 \supseteq G_1 \supseteq \cdots \supseteq G_n = \{1\}$ be a central series of G. Then $\gamma_{i+1}(G) \subseteq G_i$ for all i.*

Proof. We proceed by induction on i. The case $i = 0$ is trivial, so we assume that the result holds for some $i \geq 0$. Let $\pi_i \colon G \to G/G_i$ is the canonical map. Since $\pi_i(G_{i-1}) \subseteq Z(G/G_i)$, it follows that

$$\pi([G, G_{i-1}]) = [\pi_i(G), \pi_i(G_{i-1})] = \{1\}.$$

This implies that $[G, G_{i-1}] \subseteq \ker \pi_i = G_{i-1}$. Hence

$$\gamma_{i+1}(G) = [G, \gamma_i(G)] \subseteq [G, G_{i-1}] \subseteq G_i. \qquad \square$$

Exercise 6.20. A group is nilpotent if and only if it admits a central series.

xca:nilpotente_central

Exercise 6.21. Let G be a group. If K is a central subgroup of G such that G/K is nilpotent, then G is nilpotent.

thm:Z(nilpotent)

Theorem 6.22 (Hirsch). *Let G be a nilpotent group. If H is a non-trivial normal subgroup of G, then $H \cap Z(G) \neq \{1\}$. In particular, $Z(G) \neq \{1\}$.*

Proof. Since $\zeta_0(G) = \{1\}$ and there exists c such that $\zeta_c(G) = G$, there exists

$$m = \min\{k : H \cap \zeta_k(G) \neq \{1\}\}.$$

Since H is normal,

$$[H \cap \zeta_m(G), G] \subseteq H \cap [\zeta_m(G), G] \subseteq H \cap \zeta_{m-1}(G) = \{1\}.$$

Thus $\{1\} \neq H \cap \zeta_m(G) \subseteq H \cap Z(G)$. If $H = G$, then $Z(G) \neq \{1\}$. □

nilpotente_minimalnormal

Exercise 6.23. Let G be a nilpotent group and M be a minimal normal subgroup of G. Then $M \subseteq Z(G)$.

A subgroup M of G is **maximal normal** if it is maximal among all normal subgroups of G.

Corollary 6.24. *Let G be a non-abelian nilpotent group and A be an abelian maximal normal subgroup of G. Then $A = C_G(A)$.*

Proof. Since A is abelian, $A \subseteq C_G(A)$. Assume that $A \neq C_G(A)$. The centralizer $C_G(A)$ is normal in G. In fact, since A is normal in G,

$$gC_G(A)g^{-1} = C_G(gAg^{-1}) = C_G(A)$$

for all $g \in G$. Let $\pi\colon G \to G/A$ be the canonical map. Then $\pi(C_G(A))$ is a non-trivial normal subgroup of $\pi(G)$. Since G is nilpotent, $\pi(G)$ is nilpotent. By Hirsch's theorem, $\pi(C_G(A)) \cap Z(\pi(G)) \neq \{1\}$. Let $x \in C_G(A) \setminus A$ be such that $\pi(x)$ is central in $\pi(G)$. Note that if $g \in G$, then $gxg^{-1} \in C_G(A)$. Then $\langle A, x\rangle$ is an abelian normal subgroup of G such that $A \subsetneq \langle A, x\rangle \subsetneq G$, a contradiction. $\square$

Theorem 6.25. *Let G be a nilpotent group. The following statements hold:*

1) *Every minimal normal subgroup of G has prime order and it is central.*
2) *Every maximal subgroup of G is normal, has prime index and contains $[G,G]$.*

Proof. We first prove (1). Let N be a minimal normal subgroup of G. Since G is nilpotent, $N \cap Z(G) \neq \{1\}$ by Hirsch's theorem. It follows that $N \cap Z(G)$ is a normal subgroup of G contained in N. Thus $N = N \cap Z(G) \subseteq Z(G)$ by the minimality of N. In particular, N is abelian. Since every subgroup of N is normal in G, N is simple and therefore $N \simeq C_p$ for some prime number p.

We now prove (2). If M is a maximal subgroup, then M is normal en G by the normalizer condition. The maximality of M implies that G/M contains no non-trivial proper subgroups. Thus $G/M \simeq C_p$ for some prime number p. Since G/M is abelian, $[G,G] \subseteq M$. $\square$

The theorem does not prove the existence of maximal subgroups, see for example what happens with the additive group of rational numbers.

pro:g^n

Proposition 6.26. *Let G be a nilpotent group and H be a subgroup of G of index n. If $g \in G$, then $g^n \in H$.*

Proof. We proceed by induction on n. The case $n = 1$ is trivial. Assume that the result holds for all subgroups of index $< n$. If H is a subgroup of index n, let $H_0 = H$ and $H_{i+1} = N_G(H_i)$ for $i \geq 1$. Then H_i is normal in H_{i+1}. Since G is nilpotent, if $H_i \neq G$, then $H_i \subsetneq H_{i+1}$ by the normalizer condition. Since $(G : H)$ is finite, there exists k such that $H_k = G$. By the inductive hypothesis, since $(H_j : H_{j-1}) < n$ for all j, it follows that $x^{(H_j:H_{j-1})} \in H_{j-1}$ for all $x \in H_j$ and all j. Thus

$$g^{(G:H)} = g^{(H_k:H_{k-1})(H_{k-1}:H_{k-2})\cdots(H_1:H_0)} \in H. \qquad \square$$

Example 6.27. The nilpotency of G is needed in the previous proposition. If $G=\mathbb{S}_3$ and $H=\{\mathrm{id},(12)\}$, then $(G:H)=3$ and de índice tres. If $g=(13)$, then $g^3=(13)\notin H$.

The following tool is useful to perform induction on nilpotent groups.

lem:a[GG] **Lemma 6.28.** *Let G be a nilpotent group of class $c\geq 2$. If $x\in G$, then the subgroup $\langle x,[G,G]\rangle$ is nilpotent of class $<c$.*

Proof. Let $H=\langle x,[G,G]\rangle$. If $x\in[G,G]$, the claim holds. Assume that $x\notin[G,G]$. Note that
$$H=\{x^nc:n\in\mathbb{Z},c\in[G,G]\},$$
as $[G,G]$ is normal in G. It is enough to show that $[H,H]\subseteq\gamma_3(G)$. Let $h=x^nc,k=x^md\in H$ where $c,d\in[G,G]$. Since
$$[h,x^m]=[x^n,[c,x^m]][c,x^m]\in\gamma_4(G)\gamma_3(G)\subseteq\gamma_3(G),$$
it follows that
$$\begin{aligned}[h,k]&=[h,x^m][x^m,[h,d]][h,d]\\&=[x^n,[c,x^m]][c,x^m][x^m,[h,d]][h,d]\in\gamma_3(G).\end{aligned}$$
□

Example 6.29. Let $G=\mathbb{D}_8=\langle r,s:r^8=s^2=1,srs=r^{-1}\rangle$ be the dihedral group of order 16. Then G is nilpotent of class three and $[G,G]=\{1,r^2,r^4,r^6\}\simeq C_4$. The subgroup $\langle s,[G,G]\rangle\simeq\mathbb{D}_4$ is nilpotent of class two.

Now an application of Lemma 6.28.

thm:T(nilpotent) **Theorem 6.30.** *If G is a nilpotent group, then*
$$T(G)=\{g\in G:g^n=1\text{ para algún }n\in\mathbb{N}\}$$
is a subgroup of G.

Proof. Let $a,b\in T(G)$ and let $A=\langle a,[G,G]\rangle$ and $B=\langle b,[G,G]\rangle$, Since A and B are both nilpotent by the previous lemma, the inductive hypothesis implies that $T(A)$ is a subgroup of A and $T(B)$ is a subgroup of B. Since $T(A)$ is characteristic in A and A is normal in G, it follows that $T(A)$ is normal in G. Similarly, $T(B)$ is normal in B. We claim that every element of $T(A)T(B)$ has finite order. Indeed, if $x\in T(A)T(B)$, say $x=a_1b_1$ with a_1 of order m, then x has finite order since
$$x^m=(a_1b_1)^m=(a_1b_1a_1^{-1})(a_1^2b_1a_1^{-2})\cdots(a^{m-1}b_1a^{-m+1})b_1\in T(B).$$
This trick allows us to prove that both ab and a^{-1} have finite order. Hence $T(G)$ is a subgroup of G. □

Another application.

thm:a=b

Theorem 6.31. *Let G be a torsion-free nilpotent group and let $a,b \in G$. If $a^n = b^n$ for some $n \neq 0$, then $a = b$.*

Proof. We proceed by induction on the nilpotency class c of G. The claim holds if G is abelian. Assume that G is nilpotent of class $c \geq 1$. Since $\langle a, [G,G] \rangle$ is a nilpotent subgroup of G of nilpotency class $< c$ and $bab^{-1} = [b,a]a \in \langle a, [G,G] \rangle$, the inductive hypothesis implies that $ba = ab$, as $a^n = (bab^{-1})^n = b^n$. Thus $(ab^{-1})^n = a^n b^{-n} = 1$. Since G is torsion-free, it follows that $a = b$. □

Corollary 6.32. *Let G be a torsion-free nilpotent group. If $x,y \in G$ are such that $x^n y^m = y^m x^n$ for some $n,m \neq 0$, then $xy = yx$.*

Proof. Let $a = x$ and $b = y^n x y^{-n}$. Since $a^m = b^m$, Theorem 6.31 implies that $a = b$. Thus $xy^n = y^n x$. By using Theorem 6.31 now with $a = y$ and $b = xyx^{-1}$, we conclude that $xy = yx$. □

The following lemma is well-known. We include the proof for completeness.

lem:fg

Lemma 6.33. *Let G be a finitely generated group and H be a finite-index subgroup of G. Then H is finitely generated.*

Proof. Assume that $G = \langle g_1, \dots, g_m \rangle$. Without loss of generality we may assume that for each i there exists k such that $g_i^{-1} = g_k$. Let $\{1 = t_1, \dots, t_n\}$ be a transversal of H in G. For $i \in \{1, \dots, n\}$ and $j \in \{1, \dots, m\}$ we write

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

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

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

where $k_1, \dots, k_{s-1} \in \{1, \dots, n\}$. Thus $t_{k_s} \in H$ and hence $t_{k_s} = 1 \in H$, which implies the claim. □

thm:T(G)finito

Theorem 6.34. *Let G be a finitely generated torsion nilpotent group. Then G is finite.*

Proof. We proceed by induction on the nilpotency class c. The case $c = 1$ is true since G is abelian. Assume that the result holds for some $c \geq 1$. Since both $[G,G]$ and $G/[G,G]$ finitely generated by Lemma 6.33, nilpotent of class $< c$ and torsion groups, the inductive hypothesis implies that both $[G,G]$ and $G/[G,G]$ are finite. Thus G is finite □

We now turn out attention to finite nilpotent groups.

lem:normalizador

Lemma 6.35. *Let G be a finite group, p a prime divisor of $|G|$ and $P \in \mathrm{Syl}_p(G)$. Then $N_G(N_G(P)) = N_G(P)$.*

Proof. Let $H = N_G(P)$. Since P is normal in H, P is the unique Sylow p-subgroup of H. To prove that $N_G(H) = H$ it is enough to show that $N_G(H) \subseteq H$. Let $g \in N_G(H)$. Since $gPg^{-1} \subseteq gHg^{-1} = H$, both $gPg^{-1} \in \mathrm{Syl}_p(H)$ and H have a unique Sylow p-subgroup, so $P = gPg^{-1}$. Thus $g \in N_G(P) = H$. $\square$

thm:nilpotente:eq

Theorem 6.36. *Let G be a finite group. The following statements are equivalent:*

1) *G is nilpotent.*
2) *Every Sylow subgroup of G is normal.*
3) *G is the direct product of its Sylow subgroups.*

Proof. We prove that $1) \implies 2)$. Let $P \in \mathrm{Syl}_p(G)$. We show that P is normal in G, this means $N_G(P) = G$. By Lemma 6.35, $N_G(N_G(P)) = N_G(P)$. Now $N_G(P) = G$ by the normalizer condition.

Veamos ahora que $2) \implies 3)$. Sean $p_1, \cdots, p_k$ los factores primos de $|G|$ y para cada $i \in \{1, \ldots, k\}$ sea $P_i \in \mathrm{Syl}_{p_i}(G)$. Por hipótesis, cada P_j es normal en G. We now prove that $P_1 \cdots P_j \simeq P_1 \times \cdots \times P_j$ for all j. The case $j = 1$ is trivial. Assume that the result holds for some $j \geq 1$. Since

$$N = P_1 \cdots P_j \simeq P_1 \times \cdots \times P_j$$

is normal in G and has order coprime with $|P_{j+1}|$, it follows that $N \cap P_{j+1} = \{1\}$. Thus

$$NP_{j+1} \simeq N \times P_{j+1} \simeq P_1 \times \cdots \times P_j \times P_{j+1},$$

as P_{j+1} is normal in G. Now that we know that $P_1 \cdots P_k \simeq P_1 \times \cdots \times P_k$ is a subgroup of order $|G|$, we conclude that $G = P_1 \times \cdots \times P_k$.

Finally, to prove that $3) \implies 1)$ we note that every p-group is nilpotent and that a finite direct product of nilpotent groups is nilpotent. $\square$

xca:truco

Exercise 6.37. Let G be a finite group. If $P \in \mathrm{Syl}_p(G)$ and M is a subgroup of G such that $N_G(P) \subseteq M$, then $M = N_G(M)$.

xca:normalizadora

Exercise 6.38. Let G be a finite nilpotent group. The following statements are equivalent:

1) G is nilpotent.
2) If $H \subsetneq G$ is a subgroup, then $H \subsetneq N_G(H)$.
3) Every maximal subgroup of G is normal in G.

Exercise 6.39. Let G be a finite nilpotent group. If p is a prime dividing the order of G, then there exists a minimal normal subgroup of order p and there exists a maximal subgroup of index p.

xca:pgrupos

Exercise 6.40. Let p be a prime and G be a non-trivial group of order p^n.

1) G has a normal subgroup of order p.

2) For each $j \in \{0,\dots,n\}$ there exists a normal subgroup of order p^j.

:nilpotente_equivalencia

Exercise 6.41. Let G be a finite group. The following statements are equivalent:

1) G is nilpotent.
2) Any two elements of coprime order commute.
3) Every non-trivial quotient of G has non-trivial center.
4) If d divides $|G|$, there exists a normal subgroup of G of order d.

Theorem 6.42 (Baumslag–Wiegold). *Let G be a finite group such that $|xy| = |x||y|$ whenever x and y have coprime order. Then G is nilpotent.*

Proof. Let $p_1,\dots,p_n$ be the distinct primes dividing the order of G. For each $i \in \{1,\dots,n\}$ let $P_i \in \mathrm{Syl}_{p_i}(G)$. We claim that $G = P_1 \cdots P_n$. The non-trivial inclusion is equivalent to show that the map

$$\psi \colon P_1 \times \cdots \times P_n \to G, \quad (x_1,\dots,x_n) \mapsto x_1 \cdots x_n$$

is surjective. We first show that ψ is injective. If $\psi(x_1,\dots,x_n) = \psi(y_1,\dots,y_n)$, then

$$x_1 \cdots x_n = y_1 \cdots y_n.$$

If $y_n \neq x_n$, then $x_1 \cdots x_{n-1} = (y_1 \cdots y_{n-1}) y_n x_n^{-1}$. But $x_1 \cdots x_{n-1}$ has order coprime with p_n and $y_1 \cdots y_{n-1} y_n x_n^{-1}$ has order divisible by p_n, a contradiction. Thus $x_n = y_n$ and hence the same argument proves that ψ is injective. Since $|P_1 \times \cdots \times P_n| = |G|$, we conclude that ψ is bijective. In particular, ψ is surjective and hence $G = P_1 \cdots P_n$.

We now show that each P_j is normal in G. Let $j \in \{1,\dots,n\}$ and $x_j \in P_j$. Let $g \in G$ and $y_j = g x_j g^{-1}$. Since $y_j \in G$, we write $y_j = z_1 \cdots z_n$ with $z_k \in P_k$ for all k. Since the order of y_j is a power of p_j, it follows that $z_1 \cdots z_n$ has order a power of p_j. Thus $z_k = 1$ for all $k \neq j$ and $y_j = z_j \in P_j$. Since each Sylow subgroup is normal, G is nilpotent. □

We conclude the section with an exercise on nilpotent groups of class two.

Exercise 6.43. Let G be a group and $x, y \in G$.

1) If $[x,y] \in C_G(x) \cap C_G(y)$, entonces $[x,y]^n = [x^n,y] = [x,y^n]$ for all $n \in \mathbb{Z}$.
2) If G is nilpotent of class two, then $(xy)^n = [y,x]^{n(n-1)/2} x^n y^n$ for all $n \in \mathbb{N}$.

Exercise 6.44. Let p be an odd prime number and P be a p-group of nilpotency class ≤ 2.

1) If $[y,x]^p = 1$ for all $x, y \in P$, then $P \to [P,P]$, $x \mapsto x^p$, is a group homomorphism.
2) $\{x \in P : x^p = 1\}$ is a subgroup of P.

B

Let G be a group. If G has maximal subgroups, the Frattini subgroup $\Phi(G)$ of G is defined as the intersection of all maximal subgroups of G. Otherwise, $\Phi(G) = G$.

xca:Phi(G)char **Exercise 6.45.** If G is a group, then $\Phi(G)$ is characteristic in G.

Example 6.46. Let $G = \mathbb{S}_3$. The maximal subgroups of G are

$$M_1 = \langle(123)\rangle, \quad M_2 = \langle(12)\rangle, \quad M_3 = \langle(23)\rangle, \quad M_4 = \langle(13)\rangle.$$

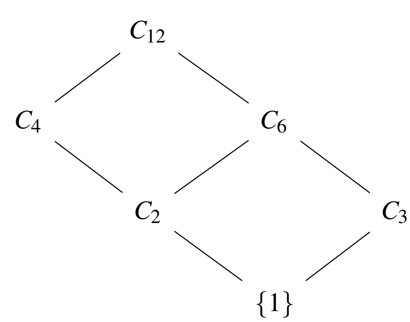
Thus $\Phi(G) = \{1\}$.

Example 6.47. Let $G = \langle g\rangle \simeq C_{12}$. The subgroups of G are

$$\{1\}, \quad \langle g^6\rangle \simeq C_2, \quad \langle g^4\rangle \simeq C_3, \quad \langle g^3\rangle \simeq C_4, \quad \langle g^2\rangle \simeq C_6, \quad G.$$

The maximal subgroups are $\langle g^3\rangle \simeq C_4$ and $\langle g^2\rangle \simeq C_6$. Hence

$$\Phi(G) = \langle g^3\rangle \cap \langle g^2\rangle = \langle g^6\rangle \simeq C_2.$$



Exercise 6.48. Compute the Frattini subgroup of $G = \mathbf{SL}_2(3)$.

lem:Dedekind **Lemma 6.49 (Dedekind).** *Let H, K and L be subgroups of G such that $H \subseteq L \subseteq G$. Then $HK \cap L = H(K \cap L)$.*

Proof. We only need to prove that $HK \cap L \subseteq H(K \cap L)$, as the other inclusion is trivial. If $x = hk \in HK \cap L$, where $x \in L$, $h \in H$ and $k \in K$, then $k = h^{-1}x \in L \cap K$ since $H \subseteq L$. Thus $x = hk \in H(L \cap K)$. □

lem:G=HPhi(G) **Lemma 6.50.** *Let G be a finite group. If H is a subgroup of G such that $G = H\Phi(G)$, then $H = G$.*

Proof. Assume that $H \neq G$. Let M be a maximal subgroup of G such that $H \subseteq M$. Since $\Phi(G) \subseteq M$, it follows that $G = H\Phi(G) \subseteq M$, a contradiction □

pro:phi(N)phi(G) **Proposition 6.51.** *Let G be a finite group and N be a normal subgroup of G. Then $\Phi(N) \subseteq \Phi(G)$.*

Proof. Since $\Phi(N)$ is characteristic in N and N is normal in G, it follows that $\Phi(N)$ is normal in G. Let M be a maximal subgroup of G such that $\Phi(N) \not\subseteq M$. Then $\Phi(N)M = G$, as $M = \Phi(N)M \supseteq \Phi(N)$ otherwise. By applying Dedekind's lemma with $H = \Phi(N)$, $K = M$ and $L = N$,

$$N = G \cap N = (\Phi(N)M) \cap N = \Phi(N)(M \cap N).$$

The previous lemma with $G = N$ and $H = M \cap N$ implies that $\Phi(N) \subseteq N \subseteq M$, a contradiction. Hence every maximal subgroup of G contains $\Phi(N)$ and therefore $\Phi(G) \supseteq \Phi(N)$. □

The Frattini subgroup can be characterized in terms of non-generators.

lemma:nongenerators **Lemma 6.52 (non-generators).** *Let G be a finite group. Then*

$$\Phi(G) = \{x \in G : \text{if } G = \langle x, Y\rangle \text{ for some } Y \subseteq G, \text{ then } G = \langle Y\rangle\}.$$

Proof. Let $x \in \Phi(G)$ be such that $G = \langle x, Y\rangle$ for some subset Y of G. If $G \neq \langle Y\rangle$, then there exists a maximal subgroup M such that $\langle Y\rangle \subseteq M$. Since $x \in M$, $G = \langle x, Y\rangle \subseteq M$, a contradiction.

Conversely, let $x \in G$ and M be a maximal subgroup of G. If $x \notin M$, then, since $G = \langle x, M\rangle$, it follows that $G = \langle M\rangle = M$, a contradiction. Thus $x \in M$ for all maximal subgroup M. Hence $x \in \Phi(G)$. □

Exercise 6.53. Let p be a prime number and G be an elementary abelian p-group. Then $\Phi(G) = \{1\}$.

theorem:Frattini **Theorem 6.54 (Frattini).** *If G is a finite group, then $\Phi(G)$ is nilpotent.*

Proof. Let $P \in \mathrm{Syl}_p(\Phi(G))$ for some prime p. Since $\Phi(G)$ is normal in G, Frattini argument implies that $G = \Phi(G)N_G(P)$. By Lemma 6.50, $G = N_G(P)$. Since Sylow subgroups of $\Phi(G)$ are normal in G, $\Phi(G)$ is nilpotent. □

exercise:G/M **Exercise 6.55.** Let G br a group and M be a normal subgroup of G that is maximal. Then G/M is cyclic of prime order.

thm:Gaschutz **Theorem 6.56 (Gaschütz).** *If G is a finite group, then $[G,G] \cap Z(G) \subseteq \Phi(G)$.*

Proof. Let $D = [G,G] \cap Z(G)$. Assume that D is not contained in $\Phi(G)$. Since $\Phi(G)$ is contained in every maximal subgroup of G, there exists a maximal subgroup M such that D is not contained in M. Thus $G = MD$. Since $D \subseteq Z(G)$, M is normal in G, since if $g = md \in G = MD$, then

$$gMg^{-1} = (md)Md^{-1}m^{-1} = mMm^{-1} = M.$$

Since G/M is cyclic of prime order, G/M is abelian. Thus $[G,G] \subseteq M$ and hence $D \subseteq [G,G] \subseteq M$, a contradiction. □

lemma:N_G(H)=H **Lemma 6.57.** *Sea G un grupo finito y sea $P \in \mathrm{Syl}_p(G)$. Sea H un subgrupo de G tal que $N_G(P) \subseteq H$. Entonces $N_G(H) = H$.*

Proof. Sea $x \in N_G(H)$. Como $P \in \mathrm{Syl}_p(H)$ y $Q = xPx^{-1} \in \mathrm{Syl}_p(H)$, gracias al segundo teorema de Sylow existe $h \in H$ tal que $hQh^{-1} = (hx)P(hx)^{-1} = P$. Entonces $hx \in N_G(P) \subseteq H$ y luego $x \in H$. □

theorem:Wielandt

Theorem 6.58 (Wielandt). *Sea G un grupo finito. Entonces G es nilpotente si y sólo si $[G,G] \subseteq \Phi(G)$.*

Proof. Supongamos que $[G,G] \subseteq \Phi(G)$. Sea $P \in \mathrm{Syl}_p(G)$. Si $N_G(P) \neq G$ entonces $N_G(P) \subseteq M$ para algún subgrupo maximal M de G. Si $g \in G$ y $m \in M$ entonces, como
$$gmg^{-1}m^{-1} = [g,m] \in [G,G] \subseteq \Phi(G) \subseteq M,$$
M es normal en G. Como además $N_G(P) \subseteq M$, el lema 6.57 implica que
$$G = N_G(M) = M,$$
una contradicción. Luego $N_G(P) = G$. Todo subgrupo de Sylow de G es normal en G y entonces G es nilpotente.

Supongamos ahora que G es nilpotente. Sea M un subgrupo maximal de G. Como M es normal en G y maximal, G/M no tiene subgrupos propios no triviales. Luego $G/M \simeq C_p$ para algún primo p. En particular G/M es abeliano y luego $[G,G] \subseteq M$. Como $[G,G]$ está contenido en todo subgrupo maximal de G, $[G,G] \subseteq \Phi(G)$. □

theorem:G/phi(G)

Theorem 6.59. *Sea G un grupo finito. Entonces G es nilpotente si y sólo si $G/\Phi(G)$ es nilpotente.*

Proof. Si G es nilpotente, entonces $G/\Phi(G)$ es nilpotente. Supongamos que $G/\Phi(G)$ es nilpotente. Sea $P \in \mathrm{Syl}_p(G)$. Como $\Phi(G)P/\Phi(G) \in \mathrm{Syl}_p(G/\Phi(G))$ y $G/\Phi(G)$ es nilpotente, $\Phi(G)P/\Phi(G)$ es un subgrupo normal de $G/\Phi(G)$. Luego, por el teorema de la correspondencia, $\Phi(G)P$ es un subgrupo normal de G. Como $P \in \mathrm{Syl}_p(\Phi(G)P)$, el argumento de Frattini (que vimos en el lema **??**) implica que
$$G = \Phi(G)PN_G(P) = \Phi(G)N_G(P)$$
pues $P \subseteq N_G(P)$. Luego $G = N_G(P)$ por el lema **??**) y entonces P es normal en G. Esto implica que G es nilpotente. □

theorem:Hall_nilpotente

Theorem 6.60 (Hall). *Sea G un grupo finito y sea N un subgrupo normal de G. Si N y $G/[N,N]$ son nilpotentes, entonces G es nilpotente.*

Proof. Como N es nilpotente, $[N,N] \subseteq \Phi(N)$ por el teorema de Wielandt (teorema 6.58). Por la proposición **??**, $[N,N] \subseteq \Phi(N) \subseteq \Phi(G)$. Por propiedad universal, existe un morfismo $G/[N,N] \to G/\Phi(G)$ sobreyectivo que hace conmutar el diagrama
$$\begin{tikzcd} G \arrow[r] \arrow[d] & G/\Phi(G) \\ G/[N,N] \arrow[ur, dashed] & \end{tikzcd}$$

Como por hipótesis $G/[N,N]$ es nilpotente, $G/\Phi(G)$ es nilpotente por el teorema **??**. Luego G es nilpotente por el teorema anterior. □

Definition 6.61. Un **conjunto minimal de generadores** de un grupo G es un conjunto X de generadores de G tal que ningún subconjunto propio de X genera a G.

Es importante observar que un conjunto minimal de generadores puede no tener cardinal mínimo.

Example 6.62. Sea $G=\langle g\rangle\simeq C_6$. Si $a=g^2$ y $b=g^3$ entonces $\{a,b\}$ es un conjunto minimal de generadores de G, aunque no tiene cardinal mínimo pues por ejemplo $G=\langle ab\rangle$.

Si p es un número primo, $\mathbb{F}_p$ denota al cuerpo de p elementos.

lemma:Burnside:minimal

Lemma 6.63. *Sea p un número primo y sea G un p-grupo finito. Entonces $G/\Phi(G)$ es un espacio vectorial sobre $\mathbb{F}_p$.*

Proof. Sea K un subgrupo maximal de G. Como G es nilpotente por la proposición **??**, K es normal en G (ejercicio 6.38). Luego $G/K\simeq C_p$ por ser un p-grupo simple.

Basta ver que $G/\Phi(G)$ es p-grupo elemental abeliano. En un p-grupo pues G es un p-grupo. Sean $K_1,\dots,K_m$ son los subgrupos maximales de G. Si $x\in G$ entonces $x^p\in K_j$ para todo $j\in\{1,\dots,m\}$ y luego $x^p\in\Phi(G)=\cap_{j=1}^m K_j$. Además $G/\Phi(G)$ es abeliano pues $[G,G]\subseteq\Phi(G)$ por ser G nilpotente por el teorema de Wielandt (teorema 6.58). □

theorem:Burnside:basis

Theorem 6.64 (Burnside). *Sea p un número primo y sea G un p-grupo finito. Si X es un conjunto minimal de generadores entonces $|X|=\dim G/\Phi(G)$.*

Proof. Vimos en el lema anterior que $G/\Phi(G)$ es un espacio vectorial sobre $\mathbb{F}_p$. Sea $\pi\colon G\to G/\Phi(G)$ el morfismo canónico y sea $\{x_1,\dots,x_n\}$ un conjunto minimal de generadores de G. Veamos que $\{\pi(x_1),\dots,\pi(x_n)\}$ es un conjunto linealmente independiente de $G/\Phi(G)$. Supongamos sin perder generalidad que $\pi(x_1)\in\langle\pi(x_2),\dots,\pi(x_n)\rangle$. Existe entonces $y\in\langle x_2,\dots,x_n\rangle$ tal que $x_1y^{-1}\in\Phi(G)$. Como G está generado por $\{x_1y^{-1},x_2,\dots,x_n\}$ y $x_1y^{-1}\in\Phi(G)$, el lema de los no-generadores (lema 6.52) implica que G también está generado por $\{x_2,\dots,x_n\}$, una contradicción a la minimalidad. Luego $n=\dim G/\Phi(G)$. □

C

Definition 6.65. Sea G un grupo finito y sea p un número primo. Se define el **p-radical** de G como el subgrupo

$$O_p(G)=\bigcap_{P\in\mathrm{Syl}_p(G)} P.$$

lemma:core:Op(G)

Lemma 6.66. *Sea G un grupo finito y sea p un número primo.*

1) *$O_p(G)$ es normal en G.*
2) *Si N es un subgrupo normal de G contenido en algún $P \in \mathrm{Syl}_p(G)$, entonces $N \subseteq O_p(G)$.*

Proof. Sea $P \in \mathrm{Syl}_p(G)$ y hagamos actuar a G en G/P por multiplicación a izquierda. Tenemos entonces un morfismo $\rho\colon G \to \mathbb{S}_{G/P}$ con núcleo

$$\begin{aligned}\ker\rho &= \{x \in G : \rho_x = \mathrm{id}\} = \{x \in G : xgP = gP\ \forall g \in G\} \\ &= \{x \in G : x \in gPg^{-1}\ \forall g \in G\} = \bigcap_{g \in G} gPg^{-1} = O_p(G).\end{aligned}$$

Luego $O_p(G)$ es normal en G.

Sea ahora N un subgrupo normal de G tal que $N \subseteq P$. Como para todo $g \in G$ se tiene $N = gNg^{-1} \subseteq gPg^{-1}$, se concluye que $N \subseteq O_p(G)$. □

Definition 6.67. Sea G un grupo finito y sean $p_1, \dots, p_k$ los factores primos de $|G|$. Se define el **subgrupo de Fitting** como el subgrupo

$$F(G) = O_{p_1}(G) \cdots O_{p_k}(G)$$

Exercise 6.68. Demuestre que $F(G)$ es characterístico en G.

Example 6.69. Sea $G = \mathbb{S}_3$. Es fácil ver que $O_2(G) = \{1\}$ y que $O_3(G) = \langle (123) \rangle$. Entonces $F(G) = \langle (123) \rangle$.

theorem:Fitting

Theorem 6.70 (Fitting). *Sea G un grupo finito. El subgrupo de Fitting $F(G)$ es normal en G y nilpotente. Además $F(G)$ contiene a todo subgrupo normal nilpotente de G.*

Proof. Por definición $|F(G)|$ es el producto de los órdenes de los $O_p(G)$. Como entonces $O_p(G) \in \mathrm{Syl}_p(F(G))$, se concluye que $F(G)$ es nilpotente por tener un p-subgrupo de Sylow normal para cada primo p. Luego $F(G)$ es nilpotente por el teorema **??**.

Sea N un subgrupo normal de G nilpotente y sea $P \in \mathrm{Syl}_p(N)$. Como N es nilpotente, P es normal en N y entonces P es el único p-subgrupo de Sylow de N. Luego P es característico en N y entonces P es normal en G. Como N es nilpotente, N es producto directo de sus subgrupos de Sylow. Luego $N \subseteq O_p(G)$ por el lema 6.66. □

corollary:Z(G)subsetF(G)

Corollary 6.71. *Sea G un grupo finito. Entonces $Z(G) \subseteq F(G)$.*

Proof. Como $Z(G)$ es nilpotente (por ser abeliano) y $Z(G)$ es normal en G, $Z(G) \subseteq F(G)$ por el teorema de Fitting. □

corollary:Fitting

Corollary 6.72 (Fitting). *Sean K y L subgrupos normales nilpotentes de un grupo finito G. Entonces KL es nilpotente.*

Proof. Por el teorema de Fitting sabemos que $K \subseteq F(G)$ y $L \subseteq F(G)$. Esto implica que $KL \subseteq F(G)$ y luego KL es nilpotente pues $F(G)$ es nilpotente. $\square$

corollary:McapF(G)

Corollary 6.73. *Sea G un grupo finito y sea N un subgrupo normal de G. Entonces $N \cap F(G) = F(N)$.*

Proof. Como $F(N)$ es característico en N, $F(N)$ es normal en G. Luego $F(N) \subseteq N \cap F(G)$ pues $F(N)$ es nilpotente. Para la otra inclusión, como $F(G)$ es normal en G, el subgrupo $F(G) \cap N$ es normal en N. Como $F(G) \cap N$ es nilpotente, $F(G) \cap N \subseteq F(N)$. $\square$

Veamos una aplicación a grupos finitos resolubles.

Theorem 6.74. *Sea G un grupo finito no trivial y resoluble. Todo subgrupo normal N no trivial contiene un subgrupo normal abeliano no trivial y este subgrupo está en realidad contenido en $F(N)$.*

Proof. Sabemos que $N \cap G^{(0)} = N \neq \{1\}$. Como G es un grupo resoluble resoluble, existe $m \in \mathbb{N}$ tal que $N \cap G^{(m)} = \{1\}$. Sea $n \in \mathbb{N}$ maximal tal que $N \cap G^{(n)}$ es no trivial. Como $[N,N] \subseteq N$ y $[G^{(n)}, G^{(n)}] = G^{(n+1)}$,

$$[N \cap G^{(n)}, N \cap G^{(n)}] \subseteq N \cap G^{(n+1)} = \{1\}.$$

Luego $N \cap G^{(n)}$ es un subgrupo abeliano de G. Como además es normal y nilpotente, $N \cap G^{(n)} \subseteq N \cap F(G) = F(N)$. $\square$

theorem:F(G)centraliza

Theorem 6.75. *Si G es un grupo finito y N es un subgrupo minimal-normal entonces entonces $F(G) \subseteq C_G(N)$.*

Proof. Por el teorema de Fitting, $F(G)$ es un subgrupo normal y nilpotente. Sea N un subgrupo minimal-normal de G. El subgrupo $N \cap F(G)$ es normal en G. Además $[F(G), N] \subseteq N \cap F(G)$. Si $N \cap F(G) = \{1\}$ entonces $[F(G), N] = \{1\}$. Si no, $N = N \cap F(G) \subseteq F(G)$ por la minimalidad de N. Como $F(G)$ es nilpotente, $N \cap Z(F(G)) \neq \{1\}$ por el teorema de Hirsch. Como $Z(F(G))$ es característico en $F(G)$ y $F(G)$ es normal en G, $Z(F(G))$ es normal en G. Como $\{1\} \neq N \cap Z(F(G))$ es normal en G, la minimalidad de N implica que $N = N \cap Z(F(G)) \subseteq Z(F(G))$ y luego $[F(G), N] = \{1\}$. $\square$

Corollary 6.76. *Sea G un grupo finito y resoluble.*

1) *Si N es un subgrupo minimal-normal entonces $N \subseteq Z(F(G))$.*
2) *Si H es un subgrupo normal entonces $H \cap F(G) \neq \{1\}$.*

Proof. Demostremos la primera afirmación. Como N es un p-grupo por el lema **??**, N es nilpotente y luego $N \subseteq F(G)$. Además $F(G) \subseteq C_G(N)$ por el teorema anterior. Luego $N \subseteq Z(F(G))$.

Demostremos ahora la segunda afirmación. El subgrupo H contiene un subgrupo minimal-normal N y $N \subseteq F(G)$. Luego $H \cap F(G) \neq \{1\}$. $\square$

Theorem 6.77. *Sea G un grupo finito.*

1) $\Phi(G) \subseteq F(G)$ *y* $Z(G) \subseteq F(G)$.
2) $F(G)/\Phi(G) \simeq F(G/\Phi(G))$.

Proof. Demostremos la primera afirmación. Como $\Phi(G)$ es normal en G y nilpotente por el teorema 6.54 y $F(G)$ contiene a todo subgrupo normal nilpotente de G (teorema 6.70), $\Phi(G) \subseteq F(G)$. Además $Z(G)$ es normal y nilpotente (por ser abeliano) y luego $Z(G) \subseteq F(G)$.

Demostremos la segunda afirmación. Sea $\pi\colon G \to G/\Phi(G)$ el morfismo canónico. Como $F(G)$ es nilpotente, $\pi(F(G))$ es nilpotente y luego

$$\pi(F(G)) \subseteq F(G/\Phi(G))$$

por el teorema 6.70. Por otro lado, sea $H = \pi^{-1}(F(G/\Phi(G)))$. Por la correspondencia, H es un subgrupo normal de G que contiene a $\Phi(G)$. Si $P \in \mathrm{Syl}_p(H)$ entonces $\pi(P) \in \mathrm{Syl}_p(\pi(H))$ pues $\pi(P) \simeq P/P \cap \Phi(G)$ es un p-grupo y además $(\pi(H) : \pi(P))$ es coprimo con p pues

$$(\pi(H) : \pi(P)) = \frac{|\pi(H)|}{|\pi(P)|} = \frac{|H/\Phi(G)|}{|P/P \cap \Phi(G)|} = \frac{(H : P)}{(\Phi(G) : P \cap \Phi(G))}$$

es un divisor de $(H : P)$, que es coprimo con p. Como $\pi(H)$ es nilpotente, $\pi(P)$ es característico en $\pi(H)$ y luego $\pi(P)$ es normal en $\pi(G) = G/\Phi(G)$. Entonces $P\Phi(G) = \pi^{-1}(\pi(P))$ es normal en G. Como $P \in \mathrm{Syl}_p(P\Phi(G))$, el argumento de Frattini del lema **??** implica que $G = \Phi(G)N_G(P)$. Luego P es normal en G por el lema **??**. Como P es nilpotente y normal en G, entonces $P \subseteq F(G)$ por el teorema 6.70. Luego $H \subseteq F(G)$ y entonces $F(G/\Phi(G)) = \pi(H) \subseteq \pi(F(G))$. □

D

Notes

Chapter 7
Solvable groups

solvable

A

For a group G we define

$$G^{(0)} = G, \quad G^{(i+1)} = [G^{(i)}, G^{(i)}] \quad i \geq 0.$$

The **derived series** of G is the sequence

$$G = G^{(0)} \supseteq G^{(1)} \supseteq G^{(2)} \supseteq \cdots$$

Each $G^{(i)}$ is a characteristic subgroup of G. We say that G is **solvable** if $G^{(n)} = \{1\}$ for some $n \in \mathbb{N}$. Clearly every abelian group is solvable. A non-abelian simple group cannot be solvable. Nilpotent groups are solvable.

Exercise 7.1. The group $\mathbf{SL}_2(3)$ is solvable.

Let p be a prime number. An **elementary abelian** p-group is a group P such that $x^p = 1$ for all $x \in P$. A subgroup M of a group G is said to be **minimal normal** if $M \neq \{1\}$, M is normal in G and the unique normal subgroup of G strictly contained in M is the trivial subgroup. Every finite group contains a minimal normal subgroup.

Example 7.2. If a normal subgroup M is minimal (with respect to the inclusion), then it is minimal normal. The converse statement is not true. The subgroup of $\mathbb{A}_4$ generated by $(12)(34)$, $(13)(24)$ and $(14)(23)$ is minimal normal in $\mathbb{A}_4$ but it is not minimal.

Example 7.3. Let $G = \mathbb{D}_6 = \langle r, s : r^6 = s^2 = 1, srs = r^{-1} \rangle$ be the dihedral group of size twelve. The subgroups $S = \langle r^2 \rangle$ and $T = \langle r^3 \rangle$ are minimal normal subgroups.

Exercise 7.4. Let $G = \mathbf{SL}_2(3)$. The unique minimal normal subgroup of G is $Z(\mathbf{SL}_2(3)) \simeq C_2$:

A subgroup H of a group G is said to be **characteristic** if $f(H) \subseteq H$ for all $f \in \mathrm{Aut}(G)$. The center $Z(G)$ and the commutator subgroup $[G,G]$ of G are both characteristic subgroups of G. Every characteristic subgroup of G is normal in G. If H is a characteristic subgroup of K and K is normal in G, then H is normal in G.

lem:minimal_normal

Lemma 7.5. *Let M be a minimal normal subgroup of G. If M is solvable and finite, then M is an elementary abelian p-group for some prime number p.*

Proof. Since M is solvable, $[M,M] \subsetneq M$. Moreover, $[M,M]$ es normal en G, as $[M,M]$ is characteristic in M and M is normal in G. Since M is minimal normal, it follows that $[M,M] = \{1\}$ and hence M is abelian. Now if M is finite, there exists a prime number p such that $P = \{x \in M : x^p = 1\}$ is a non-trivial subgroup of M. Since P is characteristic in M, the subgroup P is normal in G. Thus $P = M$. □

theorem:resoluble

Theorem 7.6. *Let G be a group.*

1) *Each subgroup H of G is solvable.*
2) *Let K be a normal subgroup of G. Then G is solvable if and only if K and G/K are both solvable.*

Proof. By induction one proves that $H^{(i)} \subseteq G^{(i)}$ for all $i \geq 0$. Let us prove the second claim. Let $Q = G/K$ and $\pi \colon G \to Q$ be the canonical map. By induction we prove that $\pi(G^{(i)}) = Q^{(i)}$ for all $i \geq 0$. The case $i = 0$ is trivial, as π is surjective. Now assume that the result holds for some $i \geq 0$. Then

$$\pi(G^{(i+1)}) = \pi([G^{(i)}, G^{(i)}]) = [\pi(G^{(i)}), \pi(G^{(i)})] = [Q^{(i)}, Q^{(i)}] = Q^{(i+1)}.$$

Assume that Q and K are both solvable. Since Q is solvable, there exists n such that $Q^{(n)} = \{1\}$. Since $\pi(G^{(n)}) = Q^{(n)} = \{1\}$, it follows that $G^{(n)} \subseteq K$. Since K is solvable, there exists m such that

$$G^{(n+m)} \subseteq (G^{(n)})^{(m)} \subseteq K^{(m)} = \{1\},$$

and hence G is solvable.

Let us now assume that G is solvable. There exists $n \in \mathbb{N}$ such that $G^{(n)} = \{1\}$. Thus Q is solvable, as $Q^n = f(G^{(n)}) = f(\{1\}) = \{1\}$. The group K is also solvable, as it is a subgroup of G. □

Example 7.7. Let $n \geq 5$. The group $\mathbb{S}_n$ is not solvable.

Exercise 7.8. Let p be a prime number and G be a finite p-group. Prove that G is solvable.

To prove Wielandt's theorem on solvable groups we need the following lemma.

lemma:4Wielandt

Lemma 7.9. *Let G be a finite group. If H and K are subgroups of G of coprime indices, then $G = HK$ and $(H : H \cap K) = (G : K)$.*

Proof. Let $D = H \cap K$. Since

$$(G:D) = \frac{|G|}{|H \cap K|} = (G:H)(H:H \cap K),$$

$(G:H)$ divides $(G:D)$. Similarly, $(G:K)$ divides $(G:D)$. Since $(G:H)$ and $(G:K)$ are coprime, $(G:H)(G:K)$ divides $(G:D)$. In particular,

$$\frac{|G|}{|H|}\frac{|G|}{|K|} = (G:H)(G:K) \leq (G:D) = \frac{|G|}{|H \cap K|}$$

and hence $|G| = |HK|$. Since

$$|G| = |HK| = |H||K|/|H \cap K|,$$

it follows that $(G:K) = (H:H \cap K)$. $\square$

The **normal closure** H^G of a subgroup H of G is the subgroup

$$H^G = \langle xHx^{-1} : x \in G \rangle$$

generated by all conjugates of H. The subgroup H^G is the smallest normal subgroup of G containing H.

Example 7.10. Let $G = \mathbb{A}_4$ and $H = \{\mathrm{id}, (12)(34)\}$. Then

$$H^G = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} \simeq C_2 \times C_2.$$

heorem:Wielandt:solvable

Theorem 7.11 (Wielandt). *Let G be a finite group and H, K and L be subgroups of G with pair-wise coprime indices. If H, K and L are solvable, then G is solvable.*

Proof. Assume the theorem is not valid and let G be a minimal counterexample. Then G is not trivial. Let N be a minimal-normal subgroup of G and $\pi\colon G \to G/N$, $g \mapsto gN$, be the canonical map. Since by definition N is non-trivial, it follows that $|G/N| < 1$. The subgroups $\pi(H) = \pi(HN)$, $\pi(K) = \pi(KN)$ and $\pi(L) = \pi(LN)$ of $\pi(G) = G/N$ are solvable. The correspondence theorem implies that the indices of $\pi(H)$, $\pi(K)$ and $\pi(L)$ in $\pi(G)$ are pair-wise coprime. By the minimality of G, the group $\pi(G)$ is solvable. If $H = \{1\}$, then $|G| = (G:H)$ is coprime with $(G:K)$ and hence $G = K$ is solvable. So we may assume that $H \neq \{1\}$. Let M be a minimal normal subgroup of H. By Lemma 7.5, M is a p-group for some prime number p. We may assume that p does not divide $(G:K)$ (if p divides $(G:K)$, then p does no divide $(G:L)$ and hence it is enough to replace K by L). There exists $P \in \mathrm{Syl}_p(G)$ such that $P \subseteq K$. By Sylow's theorem, there exists $g \in G$ such that $M \subseteq gKg^{-1}$. Since $(G:gKg^{-1}) = (G:K)$ and $(G:H)$ are coprime, Lemma 7.9 implies that $G = (gKg^{-1})H$.

We claim that all conjugate of M are included in gKg^{-1}. If $x \in G$, then $x = uv$ for some $u \in gKg^{-1}$ and $v \in H$. Since M is normal in H,

$$xMx^{-1} = (uv)M(uv)^{-1} = uMu^{-1} \subseteq gKg^{-1}.$$

In particular, $\{1\} \neq M^G \subseteq gKg^{-1}$ is solvable, as gKg^{-1} is solvable. The minimality of G implies that G/M^G is solvable. Hence G is solvable by Theorem 7.6. □

Let G be a finite group of order $p^\alpha m$ with p a prime number coprime with m. A subgroup H of G is a p-**complement** if $|H| = m$.

Example 7.12. Sea $G = \mathbb{S}_3$. Then $H = \langle (123) \rangle$ is a 2-complement and $K = \langle (12) \rangle$ is a 3-complement.

A famous theorem of Burnside states that finite groups whose order are divisible by exactly two primes are solvable.

Theorem 7.13 (Burnside). *Let p and q be prime numbers and let G be a group of order $p^\alpha q^\beta$. Then G is solvable.*

There is a quite easy proof that uses basic character theory, see for example. A non-character-theoretic proof is known but it is harder, see [39].

theorem:Hall:solvable

Theorem 7.14 (Hall). *Let G be a finite group that admits a p-complement for all primes p dividing the order of G. Then G is solvable.*

Proof. Let $|G| = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ with the p_j being distinct primes. We proceed by induction on k. If $k = 1$, then G is a p-group and the result is clear. If $k = 2$, then Burnside's theorem implies the claim. Assume now that $k \geq 3$. For each $j \in \{1,2,3\}$ let H_j be p_j-complement in G. Since $|H_j| = |G|/p_j^{\alpha_j}$, the subgroups H_j have coprime indices.

We claim that H_1 is solvable. Note that $|H_1| = p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Let p be a prime number that divides $|H_1|$ and let Q be a p-complement in G. Since $(G:H_1)$ and $(G:Q)$ are coprime, Lemma 7.9 implies that

$$(H_1 : H_1 \cap Q) = (G:Q).$$

Thus $H_1 \cap Q$ is a p-complement in H_1. Hence H_1 is solvable by the inductive hypothesis. Similarly, H_2 and H_3 are both solvable.

Since H_1, H_2 and H_3 are solvable and have coprime indices, Wielandt's theorem implies the claim. □

B

We now use Hall's theorem to obtain information related to the structure of finite braces.

thm:add_nilpotent

Theorem 7.15. *Let A be a finite brace of nilpotent type. Then the multiplicative group of A is solvable.*

Proof. Let K be the additive group of A and G be the multiplicative group of A. Assume that $|A| = p_1^{\alpha_1} \cdots p_n^{\alpha}$ for different primes numbers $p_1, \dots, p_n$. Since K is nilpotent, each $K_i \in \mathrm{Syl}_{p_j}(K)$ is normal in K, so each K_i is a left ideal of A. It follows that for each $i \in \{1, \dots, n\}$ both K_i and $\prod_{j \neq i} K_j$ are braces of coprime order. In particular, for each $i \in \{1, \dots, n\}$ there exists a subgroup of G of order coprime with p. Then G is solvable by Hall's theorem. □

Exercises

`prob:G(X,r)solvable`

7.1. Let (X, r) be a finite involutive solution. Prove that $G(X, r)$ is solvable.

Notes

Solvable groups...

In [32], Etingof, Schedler and Soloviev proved that the structure group of a finite involutive solution is always solvable.

Chapter 8
Factorizations

factorizations

A

In Chapter 4 we found that groups with an exact factorization produce braces. In this chapter we will study a different relationship between factorizations and braces.

A group G is said to be **factorized through subgroups** A and B if $G = AB$. We remark that we do not assume that $A \cap B = \{1\}$.

A group G is **metabelian** if $[G,G]$ is abelian. Thus G is metabelian if and only if there is a normal subgroup K of G such that K and G/K are abelian. The groups $\mathbb{S}_3$ and $\mathbb{A}_4$ are metabelian.

Exercise 8.1. Let G be a metabelian group.

1) If H is a subgroup of G, then H is metabelian.
2) If $f\colon G \to H$ is a group homomorphism, then $f(H)$ is metabelian.

Exercise 8.2. Prove that $\mathbf{SL}_2(3)$ is metabelian.

A straightforward calculation shows that the following formulas hold:

$$[a,bc] = [a,b]b[a,c]b^{-1},$$
$$[ab,c] = a[b,c]a^{-1}[a,c].$$

The following theorem is considered the most satisfying result about group factorization. The proof is based on a surprisingly short and smart calculation with commutators.

theorem:Ito

Theorem 8.3 (Itô). *Let $G = AB$ be a factorization of G through the abelian subgroups A and B. Then G is metabelian.*

Proof. Since $G = AB$, it follows that $AB = BA$. Let us prove that $[A,B]$ is a normal subgroup of G. Let $a, a_1, \alpha, \alpha_1 \in A$ and $b, b_1, \beta, \beta_1 \in B$ be such that $\alpha b \alpha^{-1} = b_1 a_1$, $\beta a \beta^{-1} = a_2 b_2$. Since

$$\alpha[a,b]\alpha^{-1} = a(\alpha b\alpha^{-1})a^{-1}(\alpha b^{-1}\alpha^{-1}) = ab_1a_1a^{-1}a_1^{-1}b_1^{-1} = [a,b_1] \in [A,B]$$
$$\beta[a,b]\beta^{-1} = (\beta a\beta^{-1})\beta b\beta^{-1}(\beta a^{-1}\beta^{-1})b^{-1} = a_2b_2bb_2^{-1}a_2^{-1}b^{-1} = [a_2,b] \in [A,B],$$

it follows that $[A,B]$ is a normal subgroup of G.

Now we prove that $[A,B]$ is abelian. Since

$$\beta\alpha[a,b]\alpha^{-1}\beta^{-1} = \beta[a,b_1]\beta^{-1} = (\beta a\beta^{-1})b_1(\beta a^{-1}\beta^{-1})b_1^{-1} = [a_2,b_1],$$
$$\alpha\beta[a,b]\beta^{-1}\alpha^{-1} = \alpha[a_2,b]\alpha^{-1} = a_2(\alpha b\alpha^{-1})a_2^{-1}(\alpha b\alpha^{-1}) = [a_2,b_1],$$

a direct calculation shows that

$$[\alpha^{-1},\beta^{-1}][a,b][\alpha^{-1},\beta^{-1}]^{-1} = [a,b].$$

Since two arbitrary generators of $[A,B]$ commute, the group $[A,B]$ is abelian.

Finally we note that $[G,G] = [A,B]$. Since $[A,B]$ is normal in G,

$$[a_1b_1,a_2b_2] = a_1[a_2,b_1]^{-1}a_1^{-1}a_2[a_1,b_2]a_2^{-1} \subseteq [A,B]. \qquad \square$$

Sysak found the following generalization of Itô's theorem:

Theorem 8.4 (Sysak). *If A and B are abelian subgroups of G and H is a subgroup of G contained in the set AB, then H is metabelian.*

The proof appears in [65].

There are several other interesting results in the theory of factorizable groups. Another important result that is worth mentioning is the following theorem.

Theorem 8.5 (Kegel–Wielandt). *Let G be a finite group. If there are nilpotent subgroups A and B of G such that $G = AB$, then G is solvable.*

The proof appears for example in [3, Theorem 2.4.3].

The theorem of Kegel–Wielandt turns out to be the main tool in the proof of the following result on the structure of finite braces. This proves a conjecture of Byott, see [15].

thm:mul_nilpotent

Theorem 8.6. *Let A be a finite brace with nilpotent multiplicative group. Then the additive group of A is solvable.*

Proof. Let K be the additive group of A and G be the multiplicative group of A. The group $\Gamma = K \rtimes G$ has multiplication

$$(g,\lambda_g)(h,\lambda_h) = (g+\lambda_g(h),\lambda_g\lambda_h) = (g\circ h,\lambda_{g\circ h}).$$

Let $f\colon G \to \Gamma$, $g \mapsto (g,\lambda_g)$. Then f is a group homomorphism and $f(G)$ is nilpotent. Since $\lambda(G)$ is nilpotent, the finite group $K \rtimes \lambda(G) = f(G)\lambda(G)$ is a product of nilpotent groups. By the theorem of Kegel–Wielandt, $K \rtimes \lambda(G)$ is solvable. Hence K is solvable. $\square$

B

It turns out to be interesting to study factorization of braces.

Definition 8.7. Let A be a brace and let B and C be left ideals of A. We say that A admits a *factorization* through B and C if $A = B + C$.

Note that if a brace A admits a factorization through B and C, then it follows that

$$A = B + C = C + B = B \circ C = C \circ B.$$

Now we prove an analog of Itô's theorem in the context of braces. It turns out that one needs to consider factorizations through strong left ideals. We also need the following definition:

Definition 8.8. A brace A is said to be *meta-trivial* if $A^{(2)}$ is a trivial brace.

Clearly a brace A is meta-trivial if and only there is an ideal I of A such that I and A/I are trivial as braces.

lem:calcbraces

Lemma 8.9. *Let A be a brace. For any $x, y, z \in A$ the following statements hold:*

1) $x*(y+z) = x*y+y+x*z-y$,
2) $(x \circ y)*z = x*(y*z)+y*z+x*z$.

lem:calculations

Lemma 8.10. *Let A be a brace such that $A = B + C$, where B and C are left ideals. If B and C are trivial as braces then, for any $b, \beta \in B$ and $c, \gamma \in C$, the following statements hold:*

1) $\lambda_{\beta \circ \gamma} = \lambda_{\gamma \circ \beta}$,
2) $(c+b) \circ \beta - \beta = c + b + c * \beta$,
3) $b \circ c \circ b' \circ c' = b \circ c - c \circ b = b + \lambda_b(c) - \lambda_c(b) - c \in \ker \lambda$.

Proof. To prove (1) put $c_1 = \lambda_\beta(c) \in C$ and $b_1 = \lambda_\gamma(b) \in B$. As B and C are trivial braces, $\lambda_\beta(b+c) = \lambda_\beta(b) + \lambda_\beta(c) = b + c_1$ and similarly $\lambda_\gamma(b+c) = b_1 + c$. Then $\lambda_{\beta \circ \gamma}(b+c) = b_1 + c_1 = \lambda_{\gamma \circ \beta}(b+c)$.

Let us prove (2). As B is a trivial brace, it follows from (4.2) that

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

Part (3) follows from the following computation

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

Moreover, by (1) it follows that $b\circ c\circ b'\circ c'\in\ker\lambda$. □

lem:hardworkfactoriz

Lemma 8.11. *Let A be a brace such that $A=B+C$ is a factorization through left ideals B and C. If B and C are trivial braces, then:*

1) *$B*C$ and $C*B$ are strong left ideals of A,*
2) *$B*C$ and $C*B$ are trivial braces, and*
3) *$A^{(2)}=C*B+B*C=B*C+C*B$.*

Proof. Since C is a left ideal, it follows that $B*C\subseteq C$. Let $b,\beta\in B$ and $c,\gamma\in C$. As C is trivial, it follows that

$$\begin{aligned} \lambda_{b\circ c}(\beta*\gamma) &= \lambda_b(\beta*\gamma)\\ &= \lambda_b\lambda_\beta(\gamma)-\lambda_b(\gamma)\\ &= \lambda_{b\circ\beta\circ b'}\lambda_b(\gamma)-\lambda_b(\gamma)\\ &= (b\circ\beta\circ b')*\lambda_b(\gamma)\in B*C. \end{aligned}$$

Hence $B*C$ is a left ideal and trivial as a brace.

Let $a\in A$, $b\in B$ and $c\in C$. Write $a=b_1+c_1$, with $b_1\in B$ and $c_1\in C$. Then

$$\begin{aligned} a+(b*c)-a &= a+\lambda_b(c)-c-a\\ &= -(b*a)+b*(a+c) \qquad (8.1)\\ &= -(b*(b_1+c_1))+b*(b_1+c_1+c). \end{aligned}$$ eq:7

As $B+C=C+B$, it follows that for any $\beta\in B$ and $\gamma\in C$, there exist $\beta_1\in B$ and $\gamma_1\in C$ such that $\beta+\gamma=\gamma_1+\beta_1$. Hence, for any $b\in B$ it holds that

$$b*(\beta+\gamma)=b*(\gamma_1+\beta_1)=b*\gamma_1+\gamma_1+b*\beta_1-\gamma_1=b*\gamma_1,$$

as B is trivial. Applying this on (8.1) it follows that $B*C$ is a normal subgroup of $(A,+)$. This proves (1) and (2) for $B*C$. The proof for $C*B$ is similar.

Now we show that $A^{(2)}\subseteq C*B+B*C$. Let $b,b_1\in B$ and $c,c_1\in C$. Then

$$\begin{aligned} (b\circ c)*(b_1+c_1) &= (b\circ c)*b_1+b_1+(b\circ c)*c_1-b_1\\ &= \lambda_{b\circ c}(b_1)-b_1+b_1+b*(c*c_1)+c*c_1+b*c_1-b_1\\ &= \lambda_c(b_1)-b_1+b_1+b*c_1-b_1\\ &= c*b_1+b_1+b*c_1-b_1\in C*B+B*C. \end{aligned}$$

Clearly $C*B+B*C\subseteq A^{(2)}$ and thus $A^{(2)}=C*B+B*C=B*C+C*B$. □

thm:Ito_braces

Theorem 8.12. *Let A be a brace. If $A = B + C$ is a factorization through strong left ideals B and C that are trivial as braces, then A is right nilpotent of class at most three. In particular, A is meta-trivial.*

Proof. By Lemma 8.11, $B * C$ and $C * B$ are strong left ideals of A, and both are trivial as braces. Furthermore,

$$A^{(2)} = B * C + C * B = (B * C) \circ (C * B).$$

It rests to show that $A^{(2)}$ acts trivially on A. We first show that $B * C$ acts trivially on A. For that purpose, let $b \in B$, $c \in C$ and $a \in A$. Write $a = \beta + \gamma$, where $\beta \in B$ and $\gamma \in C$. Then

$$(b * c) * (\beta + \gamma) = (b * c) * \beta + \beta + (b * c) * \gamma - \beta = (b * c) * \beta,$$

as C is a trivial brace. By Lemma 8.10(3),

$$(b \circ c - c \circ b) + \beta = (b \circ c - c \circ b) \circ \beta = (b + \lambda_b(c) - \lambda_c(b) - c) \circ \beta.$$

Since $(B, +)$ is a normal subgroup of $(A, +)$,

$$b \circ c - c \circ b = b + \lambda_b(c) - \lambda_c(b) - c = \lambda_b(c) - c + b_1$$

for some $b_1 \in B$. By Lemma 8.10(2),

$$\begin{aligned}(b \circ c - c \circ b) + \beta &= (\lambda_b(c) - c + b_1) \circ \beta \\ &= \lambda_b(c) - c + b_1 + (b * c) * \beta + \beta\end{aligned}$$

and therefore $(b * c) * \beta = 0$. Thus $B * C$ acts trivially on A. As $(C, +)$ also is a normal subgroup of $(A, +)$, it follows by symmetry that $C * B$ acts trivially on A. Hence $A^{(2)}$ acts trivially on A. ◻

Corollary 8.13. *Let A be a brace. Assume that $A = B + C$, where B and C are (not necessarily strong) left ideals, which are trivial as braces. Then A has a meta-trivial ideal I such that A/I is a trivial brace.*

Proof. By Lemma 8.11, the ideal $A^{(2)}$ has a factorization through the strong left ideals $B * C$ and $C * B$, which are trivial braces. By Theorem 8.12, $A^{(2)}$ is meta-trivial and hence the claim follows. ◻

Theorem 8.12 has application to involutive solutions.

thm:MP

Theorem 8.14. *Let (X, r) be an involutive non-degenerate (not necessarily finite) solution of the Yang–Baxter equation with $|X| \geq 2$. If the brace of abelian type $\mathscr{G}(X, r)$ admits a factorization through left ideals, which are trivial as left braces, then (X, r) is a multipermutation solution of level at most three.*

Proof. Let $A = \mathscr{G}(X, r)$ and $G = G(X, r)$. Then Theorem 8.12 yields $A^{(m)} = 0$ for some $m \leq 3$. Because $G/\operatorname{Soc}(G) \cong A$ as left braces, we get $G^{(m)} \subseteq \operatorname{Soc}(G)$, and thus $G^{(m+1)} = 0$. Hence G is a right nilpotent left brace of class at most four and, by [**?**, Proposition 6], (G, r_G) is a multipermutation solution of level at most three. Therefore, by [35, Theorem 5.15], (X,r) is a multipermutation solution of level at most three. □

This shows that properties of the involutive non-degenerate set-theoretic solution (X,r) are not completely determined by the group theory of the additive and multiplicative groups of the left brace $\mathscr{G}(X,r)$.

exa:B(8,27) **Example 8.15.** Let $X = \{1,2,3,4\}$ and $r(x,y) = (\sigma_x(y), \tau_y(x))$ be the irretractable involutive non-degenerate solution given by

$$\begin{aligned} \sigma_1 &= (34), & \sigma_2 &= (1324), & \sigma_3 &= (1423), & \sigma_4 &= (12),\\ \tau_1 &= (24), & \tau_2 &= (1432), & \tau_3 &= (1234), & \tau_4 &= (13). \end{aligned}$$

The associated left brace $\mathscr{G}(X,r)$ has additive group C_2^3 and multiplicative group D_8. Furthermore, $\mathscr{G}(X,r)$ is not right nilpotent. Hence it is impossible to decompose the left brace $\mathscr{G}(X,r)$ as in Theorem 14.20.

Example 8.16. The left brace $B(8,26)$ has the same additive and multiplicative groups as the brace $\mathscr{G}(X,r)$ of Example 8.15 but it has a factorization as in Theorem 14.20. This shows that $B(8,26)$ is right nilpotent.

Exercises

prob:decomposable **8.1.** Let A be a brace. If there exists a proper strong left ideal I, then (A, r_A) is decomposable as $A = I \cup A \setminus I$.

prob:Ito_relaxed **8.2.** Prove that the assumptions of Theorem 8.12 cannot be relaxed.

prob:Ito_version2 **8.3.** Let A be a non-zero brace that has a factorization $A = B + C$ through left ideals B and C, where both are trivial as braces. If B is a strong left ideal of A, then B or C contains a non-zero ideal I of A that acts trivially on A.

prob:mul_abelian **8.4.** Let A be a brace with abelian multiplicative group. Prove that the the additive group of A is meta-abelian.

prob:mul_cyclic **8.5.** Let A be a finite brace with cyclic multiplicative group. Prove that the the additive group of A is supersolvable.

Open problems

problem:Byott **Open problem 8.1.** Let A be a brace with solvable additive group. Is the multiplicative group of A solvable?

Notes

Theorem 8.12 was proved by Jespers, Kubat, Antwerpen and Vendramin in [42]. Exercises 8.2 and 8.3 also appear in there. One cannot expect a naive result similar to that of Kegel–Wielandt in the context of braces.

Theorem 8.6 was proved by Tsang and Qin in [66]. Exercises 8.4 and 8.5 also appear in [66].

Problem 8.1 was formulated by Byott in [15].

Chapter 9
The structure brace of a solution

structure_brace

The prove that the structure group $G(X,r)$ of a solution (X,r) is a brace, we follow the proof of Lu, Yan and Zhu. They use the language of braided groups.

Definition 9.1. A *braided group* is a pair (G,r), where G is a group with operation $m\colon G\times G\to G$, $m(x,y)=xy$, and $r\colon G\times G\to G\times G$ is a bijective map such that

1) $r(xy,z)=(\mathrm{id}\times m)r_1r_2(x,y,z)$ for all $x,y,z\in G$,
2) $r(x,yz)=(m\times\mathrm{id})r_2r_1(x,y,z)$ for all $x,y,z\in G$,
3) $r(1,x)=(x,1)$ and $r(x,1)=(1,x)$ for all $x\in G$, and
4) $m\circ r=m$.

The map r is called a *braiding operator* on G.

Proof. □

Theorem 9.2. *Let G be a group. Then G admits a braiding operator if and only if there is a brace structure on the set G with multiplicative group G.*

Proof. □

Exercises

9.1. Prove that a braiding operator is a solution.

Chapter 10
Bieberbach groups

Bieberbach

A

B

Chapter 11
Garside groups

Garside

A

In this chapter prove that the structure group of a finite involutive solution is a Garside group.

A *monoid* is a non-empty set M provided with an associative binary operation $M \times M \to M$, $(x,y) \mapsto xy$, and an identity element. A monoid M is said to be *cancellative* if

$$xy = xz \implies y = z \quad \text{and} \quad xy = zy \implies x = z$$

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

Definition 11.1. A *Garside monoid* is a pair (M,Δ), where M is a cancellative monoid such that

1) There exists a map $d\colon M \to \mathbb{N}$ such that $d(xy) \geq d(x) + d(y)$ and $d(x) \neq 0$ if $x \neq 1$.
2)
3) Δ is a Garside element of M...
4) The family of all divisors of Δ is finite.

Definition 11.2. A group G is said to be a *Garside group* if...

Structure groups of involutive solutions are Garside groups.

thm:Chouraqui **Theorem 11.3.** *Let (X,r) be an involutive solution. Then $G(X,r)$ is a Garside group.*

Proof. □

At this point it is easy to prove the following important result of Gateva–Ivanova and Van den Bergh.

thm:torsion_free **Theorem 11.4.** *Let (X,r) be an involutive solution. Then $G(X,r)$ has no torsion. In particular, $G(X,r)$ is a Bieberbach group.*

Proof. □

As a consequence we obtain the following result on linear representations of the structure group of an involutive solution.

thm:ESS **Theorem 11.5.**

Proof. □

thm:D **Theorem 11.6.**

Proof. □

Exercises

Open problems

Notes

Theorem 11.3 was proved by Chouraqui in [24]. Our proof is based on the work of Dehornoy [28] and the presentation of Cedó's survey [18].

Theorem 11.4 was proved by Gateva–Ivanova and Van den Bergh in [36] using somewhat different methods.

Chapter 12
Invariant subgroups

invariant

A

We say that a group G acts on a group K by automorphism if the (left) action

$$G \times K \to K, \quad (g,x) \mapsto g \cdot x,$$

satisfies $g \cdot (xy) = (g \cdot x)(g \cdot y)$ for all $g \in G$ and $x, y \in K$. The group

$$C_K(G) = \{x \in K : g \cdot x = x \text{ for all } g \in G\}$$

acts on the set of G-orbits by left multiplication. Indeed, if $x \in K$ and $c \in C_K(G)$, then $g \cdot c = c$ for all $g \in G$. Thus

$$\begin{aligned} c(G \cdot x) &= \{c(g \cdot x) : g \in G\} \\ &= \{(g \cdot c)(g \cdot x) : g \in G\} = \{g \cdot (cx) : g \in G\} = G \cdot (cx). \end{aligned}$$

The following theorem goes back to Deaconescu and Walls [27]. Our proof is that of Isaacs, see [40].

thm:DeaconescuWalls

Theorem 12.1 (Deaconescu–Walls). *Let the group G acts by automorphism on a finite gorup K. Let $C = C_K(G)$ and $N = C \cap [G,K]$, where $[G,K]$ is the subgroup of K generated by $[g,x] = (g \cdot x)x^{-1}$ for all $g \in G$ and $x \in K$. Then the index $(C : N)$ divides the number of G-orbits of K.*

Proof. The group C acts by left multiplication on the set Ω of G-orbits on K. Let $X = G \cdot x \in \Omega$ be an orbit and C_X be the stabilizer of X in C de X. If $c \in C_X$, then $cX = X$. In particular, if $c \in C_X$, then $cx = g \cdot x$ for some $g \in G$. Thus

$$c = (g \cdot x)x^{-1} = [g,x] \in [G,K]$$

and hence $C_X \subseteq N$.

To prove that $(C : N)$ divides the size of Ω, decompose Ω as a disjoint union of C-orbits. Then it is enough to show that $(C : N)$ divides the size of each C-orbit. If

$X \in \Omega$, then $C \cdot X$ has size

$$(C : C_X) = (C : N)(N : C_X).$$

Thus $(C : N)$ divides the size of $C \cdot X$. $\square$

cor:Z(K)subset[K,K]

Corollary 12.2. *Let K be a non-trivial finite group with k conjugacy classes. If $|Z(K)|$ and k are coprime, then $Z(K) \subseteq [K,K]$.*

Proof. Let the group K acts on K by conjugation, which is an action by automorphism. Deaconescu–Walls' theorem implies that $(Z(K) : Z(K) \cap [K,K])$ divides k. Since k and $|Z(K)|$ are coprime, it follows that $Z(K) = Z(K) \cap [K,K] \subseteq [K,K]$. $\square$

Let K be a group and $f \in \operatorname{Aut}(K)$. Then f is **central** if $f(x)x^{-1} \in Z(K)$ for all $x \in K$. Note that $f \in \operatorname{Aut}(K)$ is central if and only if $f \in C_{\operatorname{Aut}(K)}(\operatorname{Inn}(K))$.

Corollary 12.3. *Let K be a finite group with k conjugacy classes and c central automorphisms. If $\gcd(|K|, kc) = 1$, then $[K,K] = Z(K)$.*

Proof. By Corollary 12.2, $Z(K) \subseteq [K,K]$.

Let us prove that $Z(K) \supseteq [K,K]$. Let $G = C_{\operatorname{Aut}(K)}(\operatorname{Inn}(K))$. Since $\gcd(|K|, kc) = 1$ and $(C_K(G) : C_K(G) \cap [G,K])$ divides c, Deaconescu–Walls' theorem, it follows that $C_K(G) = C_K(G) \cap [G,K]$. Since $[K,K] \subseteq C_K(G)$, as

$$a \cdot [x,y] = [(a \cdot x)x^{-1}x, (a \cdot y)y^{-1}y] = [x,y]$$

for all $a \in G$, $x, y \in K$ and $[G,K] \subseteq Z(K)$, we conclude that

$$[K,K] \subseteq C_K(G) = C_K(G) \cap [G,K] \subseteq [G,K] \subseteq Z(K). \qquad \square$$

Corollary 12.4. *Let p be a prime number. If K is a group with p conjugacy classes, then $Z(K) \subseteq [K,K]$ or $|K| = p$.*

Proof. Let K acts on K by conjugation. Since every element of $C = Z(K)$ form a conjugacy class, $|C| \leq p$. If $|C| = p$, then $K = C = Z(K)$ has p elements. Otherwise, $\gcd(|C|, p) = 1$ and hence $C \subseteq N = [K,K]$. $\square$

B

In this section we will develop Sylow theory for invariant subgroups. This will be used in the next section.

Lemma 12.5 (Glauberman). *Let G and K be finite groups of coprime order, where at least one of G or K is solvable. Assume that G acts on K by automorphisms and that G acts on a set Ω, K acts transitively on Ω and*

$$(g \cdot x) \cdot (g \cdot \omega) = g \cdot (x \cdot \omega)$$

for all $g \in G$, $x \in K$ and $\omega \in \Omega$. The following statements hold:

1) *There exists a G-invariant element of Ω.*
2) *If $\omega, \omega \in \Omega$ are G-invariant elements, then $c \cdot \omega = \omega_1$ for some $c \in C_K(G)$.*

By Feit–Thompson's theorem, the solvability of G or K is not really needed since at least one of $|G|$ or $|K|$ is of odd order.

Proof of Glauberman's lemma. We demonstrate the first claim. Let $\Gamma = K \rtimes G$. Each $\gamma \in \Gamma$ can be written uniquely as $\gamma = xg$ for $x \in K$ and $g \in G$. Thus Γ acts on Ω by

$$(xg) \cdot \omega = x \cdot (g \cdot \omega), \quad x \in K, g \in G, \omega \in \Omega.$$

To prove that this is an action we use the compatibility condition to compute

$$\begin{aligned}(xg) \cdot ((x_1 g_1) \cdot \omega) &= (xg) \cdot (x_1 \cdot (g_1 \cdot \omega)) \\ &= x \cdot (g \cdot (x_1 \cdot (g_1 \cdot \omega))) = x \cdot ((g \cdot x_1) \cdot (g \cdot (g_1 \cdot \omega)) \\ &= (x(g \cdot x_1)) \cdot ((gg_1) \cdot \omega) = (x(g \cdot x_1)(gg_1)) \cdot \omega.\end{aligned}$$

Let $\omega \in \Omega$ nd $U = \Gamma_\omega$ be the stabilizer of ω in Γ. Let $\gamma \in \Gamma$. Since K acts transitively on Ω, there exists $x \in K$ such that $\gamma \cdot \omega = x \cdot \omega$. Thus $\gamma^{-1} x \in U$ and hence $x \in \gamma U \subseteq \Gamma U = \Gamma$.

Since K is normal in Γ, it follows that $U \cap K$ is normal in U. Moreover,

$$(U : U \cap K) = (KU : K) = (\Gamma : K) = |G|$$

is coprime with $|U \cap K|$. By Schur–Zassenhaus' theorem, there exists a complement H of $U \cap K$ in U. Since

$$|H| = (U : U \cap K) = |G|,$$

it follows that H is also a complement of K in Γ. Since G is a complement of K in Γ, Schur–Zassenhaus' theorem states that H and G are conjugate in Γ, this means $G = \gamma H \gamma^{-1}$ for some some $\gamma \in \Gamma$. Since $H \subseteq U$, it follows that H stabilizes ω and hence

$$G = \gamma H \gamma^{-1} = \gamma H_\omega \gamma^{-1} = H_{\gamma \cdot \omega}.$$

In particular, $\gamma \cdot \omega$ is a G-invariant element.

Let us prove the second claim. Let $\omega, \omega_1 \in \Omega$ be G-invariant elements. By assumption, K acts transitively on Ω and thus the set

$$X = \{x \in K : x \cdot \omega = \omega_1\}$$

is non-empty.

Claim. The groups G acts on X.

If $x \in X$, then $x \cdot \omega = \omega_1$. By applying $g \in G$ to this equality we obtain that $g \cdot (x \cdot \omega) = g \cdot \omega_1$. By the compatibility condition and using that ω and ω_1 are both G-invariant elements,

$$(g \cdot x) \cdot \omega = (g \cdot x) \cdot (g \cdot \omega) = g \cdot (x \cdot \omega) = g \cdot \omega_1 = \omega_1.$$

This proves that $G \cdot X \subseteq X$ and hence G acts on X.

Claim. There exists a G-invariant element of X. (This completes the proof, as if $x \in X$ is G-invariant, then $x \in K$ is such that $x \cdot \omega = \omega_1$ and $g \cdot x = x$ for all $g \in G$, i.e. $x \in C_K(G)$.)

Let $H = K_{\omega_1}$. Note that H is a subgroup of K. The group H acts transitively on X by left multiplication: if $h \in H$ and $x \in X$, then

$$(hx) \cdot \omega = h \cdot (x \cdot w) = h \cdot \omega_1 = \omega_1.$$

The action of G on K restricts to H and hence G acts on H by automorphisms. The orders of G and H are coprime and either G or H is solvable. The group G acts on X and . The compatiblity condition holds:

$$g \cdot (h \cdot x) = g \cdot (hx) = (g \cdot h)(g \cdot x) = (g \cdot h) \cdot (g \cdot x),$$

as G acts on K by automorphisms. Hence the first part of the lemma implies the existence of a G-invariant element of X. □

We now prove Sylow's theorems for invariant subgroups.

Theorem 12.6. *Let G act by automorphisms on K, where G and K are finite groups of coprime order. Assume that G and K have coprime orders and that at least one of G or K is solvable. Let p be a prime number.*

1) *There exists a Sylow p-group of K which is G-invariant.*
2) *If S and T are G-invariant Sylow p-subgroups, then there exists $c \in G_K(G)$ such that $cSc^{-1} = T$.*

Proof. Let us prove the first claim. By Sylow's theorems, the group K acts transitively by conjugation on the non-empty set $\Omega = \mathrm{Syl}_p(K)$. Since G acts on K by automorphisms, G acts on Ω. Let us check the compatibility condition. Since $g \cdot P = gPg^{-1} \in \Omega$, K acts by conjugation on Ω and G acts by automorphisms on K,

$$(g \cdot x) \cdot (g \cdot P) = (g \cdot x)(gPg^{-1})(g \cdot x)^{-1} = g \cdot (xPx^{-1}) = g \cdot (x \cdot P).$$

The first part of Glauberman's lemma implies that there exists a Sylow p-subgroup of K that is G-invariant.

Let us now prove the second claim. Let S and T be G-invariant Sylow p-subgroups of K, so S and T are G-invariant elements of Ω. By the second part of Glauberman's lemma, there exits $c \in C_K(G)$ such that $c \cdot S = cSc^{-1} = T$. □

C

Let a group G acts on K by automorphisms. The subgroup

$$[G,K] = \langle (g \cdot x)x^{-1} : g \in G, x \in K \rangle$$

of K is normal in K. Moreover,

$$C_G(K) = \{g \in G : g \cdot x = x \text{ for all } x \in K\}$$

is a subgroup of G.

Recall G can be identified with a subgroup of the semidirect product $K \rtimes G$ and K can be identified by a normal subgroup of $K \rtimes G$.

A subgroup H of K is G**-invariant** if $g \cdot H \subseteq H$ for all $g \in G$. For example, $[G,K]$ is G-invaraint, as

$$g_1 \cdot [g,x] = [g_1 g g_1^{-1}, g_1 \cdot x]$$

for all $g, g_1 \in G$ and $x \in K$.

Note that if G acts trivially on K, i.e. $g \cdot x = x$ for all $g \in G$ and $x \in K$, then $[G,K] = \{1\}$.

If H is a G-invariant subgroup of K, then G permutes the cosets of H in K. If, moreover, H is normal in K, then G acts on K/H by automorphisms. This is the **induced action** of G on K/H. Let $\pi \colon K \to K/H$ be the canonical map. Then

$$\pi(g \cdot x) = (g \cdot x)H = g \cdot (xH) = g \cdot \pi(x)$$

for all $g \in G$ and $x \in K$. Moreover,

$$\pi([g,x]) = \pi((g \cdot x)x^{-1}) = \pi(g \cdot x)\pi(x)^{-1} = (g \cdot \pi(x))\pi(x)^{-1} = [g, \pi(x)].$$

Exercise 12.7. Let G acts on K by automorphisms. Then $[G,K]$ is the unique smallest G-invariant subgroup of K such that the induced action of G on $K/[G,K]$ is trivial.

Proposition 12.8. *Let H be a subgroup of K. Each right coset of H in K is G-invariant if and only if $[G,K] \subseteq H$. In particular, $[G,K]$ is the unique smallest subgroup of K with the property that all its right cosets are G-invariant.*

Proof. Assume first that all right cosets of H in K are G-invariant. If $g \in G$ and $x \in K$, then $g \cdot x \in g \cdot (Hx) = Hx$ and hence $[g,x] = (g \cdot x)x^{-1} \in H$. This implies that $[G,K] \subseteq H$. Conversely, assume that $[G,K] \subseteq H$. Then every right coset of H in K is a disjoint union of right cosets of $[G,K]$ in K. Since all these right cosets are G-invariant, it follows that each right coset of H is also G-invariant. $\square$

The bijective map $xH \mapsto Hx^{-1}$ can be used to prove that all right cosets of H in K are G-invariant if and only if all left cosets of H in K are G-invariant.

An action is said to be **faithful** if $g \cdot x = x$ for all x implies that $g = 1$. Note that if the action is faithful, then $C_G(K) = \{1\}$.

The **kernel** of an action is the (normal) subgroup N of elements that act trivially. In this case, the quotient group G/N acts by $\pi(g) \cdot x = g \cdot x$ and the action is faithful. Note that the kernel of the action is the subgroup $C_G(K)$ of $K \rtimes G$. Note that $C_G(K)$

is isomorphic to the largest subgroup N of G such that $[N,K]=\{1\}$. If $N=C_G(K)$, then N is normal in G. In this case, the quotient group G/N acts on K by $g\cdot x=\pi(g)\cdot x$.

It will be convenient to introduce the following notaiton.

Let $[G,\dots,G,K]_1=[G,K]$ and $[G,\dots,G,K]_{m+1}=[G,\dots,G,[G,K]]_m$ for $m\geq 1$. Note that

$$[G,\dots,G,K]_m=[\underbrace{G,\dots,G}_{m\text{-copies}},K]$$

for $m\geq 1$.

Theorem 12.9. *Let G act by automorphisms on K. If $[G,\dots,G,K]_m=\{1\}$, then $G^{(m-1)}\subseteq C_G(K)$. In particular, if the action is faithful, then G is solvable and its derived series has length $\leq m-1$.*

Proof. Let us prove that $G^{(m-1)}\subseteq C_G(K)$ for all m. We proceed by induction on m. If $m=1$, then $[G,K]=\{1\}$ by assumption and thus $G^{(0)}=G=C_G(K)$. Assume now that the result holds for some $m\geq 1$. L et $L=[G,K]$. Then

$$\{1\}=[G,\dots,G,K]_m=[G,\dots,G,L]_{m-1}.$$

Since L is G-invariant, G acts on L. By the inductive hypothesis, $G^{(m-2)}\subseteq C_G(L)$, which implies that $[G^{(m-2)},L]=\{1\}$. Thus

$$[G^{(m-2)},[G^{(m-2)},K]]\subseteq[G^{(m-2)},[G,K]]=[G^{(m-2)},L]=\{1\}.$$

Moreover, since $[G^{(m-2)},K]=[K,G^{(m-2)}]$, it follows that

$$[G^{(m-2)},[K,G^{(m-2)}]]=\{1\}.$$

The three-subgroups Lemma with $X=Y=G^{(m-2)}$ and $Z=K$ implies that

$$\{1\}=[K,[G^{(m-2)},G^{(m-2)}]]=[K,G^{(m-1)}].$$

Hence $G^{(m-1)}\subseteq C_G(K)$. In particular, if the action is faithful, then $C_G(K)=\{1\}$ and the claim follows. $\square$

Exercise 12.10. Let G acts faithfully on K by automorphisms. If $[G,[G,K]]=\{1\}$, then G is abelian.

Theorem 12.11 (Hall). *Let G be a finite group that acts faithfully on a finite group K. If $[G,\dots,G,K]_m=\{1\}$ for some m, then G is nilpotent.*

Proof. We proceed by induction on $|K|$. We may assume that K is non-trivial. Let

$$G=\gamma_1(G)\supseteq\gamma_2(G)\supseteq\cdots\supseteq\gamma_n(G)\supseteq\cdots$$

be the lower central series of G. Since G is finite, this sequence stabilizes. Let $n\in\mathbb{N}$ be the smallest positive integer such that $\gamma_n(G)=\gamma_{n+k}(G)$ for all k.

Claim. $[G,K] \neq K$.

In fact, if $[G,K]=K$, then

$$\{1\} = [\underbrace{G,\dots,G}_{m},K]_m = [\underbrace{G,\dots,G}_{m-1},[G,K]] = \cdots = [G,K] = K,$$

a contradiction.

Claim. $\gamma_n(G)$ acts trivially on K.

In this case, if the action is faithful, then $\gamma_n(G)=\{1\}$ and hence G is nilpotent. By assumption,

$$\{1\} = [\underbrace{G,\dots,G}_{m},K] = [\underbrace{G,\dots,G}_{m-1},[G,K]].$$

Since $[G,K]$ is a proper G-invariant subgroup of K, the inductive hypothesis implies that $\gamma_n(G)$ acts trivially on $[G,K]$ and hence $[\gamma_n(G),[G,K]]=\{1\}$.

In order to use the three-subgroups lemma, we need to show that

$$[G,[K,\gamma_n(G)]] = \{1\}.$$

This is tricky, we need to find a non-trivial normal subgroup C of K such that G acts trivially on C. With this subgroup we proceed as follows. Let $\pi\colon K \to K/C$ be the canonical map. Since $|K/C|<|K|$ and

$$[G,\dots,G,\pi(K)] = \pi([G,\dots,G,K]) = \{1\},$$

the inductive hypothesis implies that

$$\{1\} = [\gamma_n(G),\pi(K)] = \pi([\gamma_n(G),K]).$$

Thus $[K,\gamma_n(G)] = [\gamma_n(G),K] \subseteq C$. In particular,

$$[G,[K,\gamma_n(G)]] = [G,[\gamma_n(G),K]] = \{1\},$$

as G acts trivially on C.

Let $C = C_{[\gamma_n(G),K]}(G)$. Clearly C is a subgroup of K and G acts trivially on C. Since the group $\gamma_n(G)$ acts trivially on $[G,K]$, it follows that $[\gamma_n(G),[G,K]]=\{1\}$. Thus

$$[K,[\gamma_n(G),[G,K]] = [K,\{1\}] = \{1\}$$

and hence, since $[G,K]$ is normal in K, it follows that

$$[\gamma_n(G),[[G,K],K]] \subseteq [\gamma_n(G),[G,K]] = \{1\}.$$

By the three-subgroups lemma with $X=K$, $Y=\gamma_n(G)$ and $Z=[G,K]$,

$$[[G,K],[\gamma_n(G),K]] = [[G,K],[K,\gamma_n(G)]] = \{1\}.$$

By definition, $C \subseteq [\gamma_n(G), K]$ and $[C, G] = \{1\}$. Thus

$$[C, [G, K]] \subseteq [[\gamma_n(G), K], [G, K]] = \{1\}$$

and

$$[K, [C, G]] = [K, \{1\}] = \{1\}.$$

By using the three-subgroups lemma with $X = K$, $Y = C$ and $Z = G$, it follows that $[G, [C, K]] = \{1\}$, so G centralizes $[C, K]$. Since $C \subseteq [\gamma_n(G), K]$ and $[\gamma_n(G), K]$ is a normal subgroup of K, it follows that $[C, K] \subseteq [\gamma_n(G), K]$. But

$$[C, K] \subseteq C_{[\gamma_n(G), K]}(G) = C$$

and therefore C is normal in G. □

For the next result we need a lemma.

lem:[G,K]abelian

Lemma 12.12. *Let G act on K by automorphisms. If $[G, [G, K]] = \{1\}$, then $[G, K]$ is abelian.*

Proof. Since $[G, [G, K]] = \{1\}$, it follows that $[K, [[G, [G, K]]] = \{1\}$. Moreover, $[G, K]$ is normal in K and thus

$$[G, [[G, K], K]] \subseteq [G, [G, K]] = \{1\}.$$

The three-subgroups lemma with $X = K$, $Y = G$ and $Z = [G, K]$ implies that

$$\{1\} = [[G, K], [G, K]],$$

so the commutator subgroup of the group $[G, K]$ is trivial. This means that $[G, K]$ is abelian. □

thm:[G,K]_pgroup

Theorem 12.13. *Let p be a prime number and G be a p-group that acts by automorphisms on a finite group K. If $[G, \dots, G, K]_m = \{1\}$ for some m, then $[G, K]$ is a p-group.*

Proof. We proceed by induction on $|K|$. We may assume that $K \neq \{1\}$. Then, since $[G, \dots, G, K] = \{1\}$, it follows that $[G, K] \neq K$. Let $L = [G, K]$. Then L is a G-invariant proper normal subgroup of K. Since

$$[L, \dots, L, K] \subseteq [G, \dots, G, K] = \{1\},$$

the inductive hypothesis on L implies that $[G, L]$ is p-group. Note that $[G, L]$ is a normal subgroup of L. Then $[G, L] \subseteq O_p(L)$ and since $O_p(L)$ is characteristic in L and L is normal in K, it follows that $O_p(L)$ is normal in K. Let $\pi\colon K \to K/O_p(L)$ be the canonical map. Since $[G, L] \subseteq O_p(L)$, the group G acts trivially on $\pi(L)$. Now

$$[\pi(G), K] = \pi([G, K]) = \pi(L)$$

implies that G acts trivially on $\pi(G)/\pi(L)$. $\boxed{?}$ □

Theorem 12.14. *Let the finite group G act on a finite group K by automorphisms. If $[G,\dots,G,K]_m = \{1\}$ for some m, then $[G,K]$ is nilpotent.*

Proof. We proceed by induction on $|G|$. If $G = \{1\}$, then $[G,K] = \{1\}$ and there is nothing to demonstrate. So we may assume that $G \neq \{1\}$. Let G_1 be a proper subgroup of G. Since

$$[G_1,\dots,G_1,K] \subseteq [G,\dots,G,K] = \{1\},$$

the inductive hypothesis implies that $[G_1,K]$ is nilpotent. Since $[G_1,K]$ is a normal subgroup of K, $[G_1,K] \subseteq F(K)$ and thus G_1 acts trivially on the quotient $K/F(K)$. $\boxed{?}$ □

C

Let G be a finite group and $\sigma \in \mathrm{Aut}(G)$. The σ-orbit of an element $g \in G$ is defined as the set

$$O(\sigma,g) = \{\sigma^j(g) : j \in \mathbb{Z}\} = \{\sigma^j(g) : \sigma_j \in \langle\sigma\rangle\}.$$

We say that $O(\sigma,g)$ is a **faithful orbit** if $|O(\sigma,g)| = |\sigma|$.

Lemma 12.15. *Let G be a finite group and p be a prime number such that p^2 divides $|\sigma|$. Then σ admits a faithful orbit if and only if σ^p admits a faithful orbit.*

Lemma 12.16. *Let N be a normal subgroup of G and $\sigma \in \mathrm{Aut}(G)$. If $\sigma|_N = \mathrm{id}$, then σ induces the identity in $G/C_G(N)$.*

Proof. Let $g \in C_G(M)$, $n \in N$ and $x \in G$. We first prove that the subgroup $C_G(N)$ is normal in G. In fact,

$$xgx^{-1}n = xg(x^{-1}nx)x^{-1} = x(x^{-1}nx)gx^{-1} = nxgx^{-1}.$$

We now prove that $C_G(N)$ is σ-invariant. Since $\sigma(n) = n$,

$$[\sigma(g),n] = \sigma(g)n\sigma(g)^{-1}n^{-1} = \sigma(gng^{-1}n^{-1}) = \sigma(1) = 1.$$

Since N is normal in G,

$$xnx^{-1} = \sigma(xnx^{-1}) = \sigma(x)\sigma(n)\sigma(x)^{-1} = \sigma(x)n\sigma(x)^{-1}$$

and hence $x^{-1}\sigma(x) \in C_G(N)$. Therefore the homomorphism on $C/C_G(N)$ induced by σ satisfies

$$\sigma(xC_G(N)) = \sigma(x)C_G(N) = xC_G(N)C_G(N) = xC_G(N).$$ □

D

Definition 12.17. Let A be a brace. One defines $A^1 = A$ and for $n \geq 1$

$$A^{n+1} = A * A^n = \langle a * x : a \in A, x \in A^n \rangle_+.$$

The sequence $A^1 \supseteq A^2 \supseteq A^3 \supseteq \cdots \supseteq A^n \supseteq \cdots$ is the *left series* of A.

pro:left_series

Proposition 12.18. *Let A be a brace. Each A^n is a left ideal of A.*

Proof. We proceed by induction on n. The case $n = 1$ is trivial, so we may assume that the result is true for some $n \geq 1$. Let $a, b \in A$ and $x \in A^n$. By the inductive hypothesis, $\lambda_a(x) \in A^n$ and hence

$$\lambda_a(b * x) = (a \circ b \circ a') * \lambda_a(x) \in A^{n+1},$$

where the equality follows by (**??**). This implies that $\lambda_a(A^{n+1}) \subseteq A^{n+1}$. Thus the result follows. $\square$

Definition 12.19. A brace A is said to be *left nilpotent* if $A^m = \{0\}$ for some $m \geq 1$.

Some basic properties of left nilpotent braces appear in Exercises 12.1–12.3.

pro:IcapFix

Proposition 12.20. *Let A be a left nilpotent brace and I be a non-zero left ideal of A. Then $I \cap \mathrm{Fix}(A) \neq \{0\}$. In particular,* $\mathrm{Fix}(A) \neq \{0\}$.

Proof. Let $m = \max\{k : I \cap A^k \neq \{0\}\}$. Since $A * (I \cap A^m) \subseteq I \cap A^{m+1} = \{0\}$, it follows that there exists a non-zero $x \in I \cap A^m$ such that $a * x = 0$ for all $a \in A$. Thus $0 \neq x \in \mathrm{Fix}(A) \cap I$. For the second claim, apply the first case with $I = A$. $\square$

Let A be a brace. Let $A^{[1]} = A$ and for $n \geq 1$ let $A^{[n+1]}$ be the additive subgroup of A generated by elements from $\{A^{[i]} * A^{[n+1-i]} : 1 \leq i \leq n\}$. One easily proves by induction that $A^{[k]} \supseteq A^{[k+1]}$ for all $k \geq 1$.

pro:Smoktunowicz

Proposition 12.21. *Let A be a brace. Each $A^{[n]}$ is a left ideal of A.*

Proof. Each $A^{[n]}$ is a subgroup of $(A, +)$. Since $A * A^{[n]} \subseteq A^{[n+1]} \subseteq A^{[n]}$, the claim follows from Proposition 4.40. $\square$

There exists a brace A such that $A^{[n]} = A^{[n+1]} \neq \{0\}$ for some positive integer n and $A^{[n+2]} = \{0\}$.

exa:funny

Example 12.22. Let

$$G = \langle r, s : r^8 = s^2 = 1, srs = r^7 \rangle \simeq \mathbb{D}_{16},$$
$$K = \langle a, b : 8a = 2b = 0, a + b = b + a \rangle \simeq \mathbb{Z}/(8) \times \mathbb{Z}/(2).$$

The group G acts by automorphisms on K via

$$r\cdot a=a+b,\quad r\cdot b=4a+b,\quad s\cdot a=3a,\quad s\cdot b=4a+b.$$

A direct calculation shows that the map $\pi\colon G\to K$ given by

$$\begin{array}{cccc}
1\mapsto 0, & r\mapsto a, & r^2\mapsto 2a+b, & r^3\mapsto 7a+b,\\
r^4\mapsto 4a, & r^5\mapsto 5a, & r^6\mapsto 6a+b, & r^7\mapsto 3a+b,\\
rs\mapsto 6a, & r^2s\mapsto 7a, & r^3s\mapsto b, & r^4s\mapsto 5a+b,\\
r^5s\mapsto 2a, & r^6s\mapsto 3a, & r^7s\mapsto 4a+b, & s\mapsto a+b,
\end{array}$$

is a bijective 1-cocycle. Therefore there exists a brace A with additive group isomorphic to K and multiplicative group isomorphic to G. The addition of A is that of K and the multiplication is given by

$$x\circ y=\pi(\pi^{-1}(x)\pi^{-1}(y)),\quad x,y\in K.$$

Since

$$\begin{aligned}
a*a&=-a+a\circ a-a=-a+(2a+b)-a=b,\\
(5a+b)*a&=-(5a+b)+(5a+b)\circ a-a=-(5a+b)+b-a=2a,
\end{aligned}$$

it follows that $A^{[2]}$ contains $\langle 2a,b\rangle_+=\{0,2a,4a,6a,b,2a+b,4a+b,6a+b\}$, the additive subgroup of $(A,+)$ generated by $2a$ and b. Therefore $A^{[2]}=\langle 2a,b\rangle_+$ since $A^{[2]}\neq A$. Routine calculations prove that

$$A^{[3]}=\{0,2a+b,4a,6a+b\},\qquad A^{[4]}=A^{[5]}=\{0,4a\},\qquad A^{[6]}=\{0\}.$$

Definition 12.23. For a brace A let $\ell_1(a)=a$ and $\ell_{k+1}(a)=a*\ell_k(a)$ for $n\geq 1$. The brace A is said to be *left nil* if there exists a positive integer n such that $\ell_n(a)=0$ for all $a\in A$.

Definition 12.24. For a brace A let $\rho_1(a)=a$ and $\rho_{k+1}(a)=\rho_k(a)*a$ for $n\geq 1$. The brace A is said to be *right nil* if there exists a positive integer n such that $\rho_n(a)=0$ for all $a\in A$.

Definition 12.25. A brace A is said to be *strongly nilpotent* if there is a positive integer n such that $A^{[n]}=0$.

Definition 12.26. A brace A is said to be *strongly nil* if for every $a\in A$ there is a positive integer $n=n(a)$ such that any $*$-product of n copies of a is zero.

We first prove that if both groups of a finite brace A are nilpotent, then A can be decomposed as a direct product of braces of prime-power size.

sum **Lemma 12.27.** *Let A be a brace such that the additive group is a direct sum of ideals I_1,I_2, that is $A=I_1+I_2$ and $I_1\cap I_2=\{0\}$. Then the map $f:A\to I_1\times I_2$ defined by $f(a_1+a_2)=(a_1,a_2)$, for all $a_1\in I_1$ and $a_2\in I_2$, is an isomorphism of braces.*

Proof. The operations of the brace $I_1 \times I_2$ are defined component-wise. Clearly f is an isomorphism of the additive groups of A and $I_1 \times I_2$. Let $a_1 \in I_1$ and $a_2 \in I_2$. Since I_1 and I_2 are ideals we have that

$$a_1 + a_2 - a_1 - a_2, a_1 * a_2, a_2 * a_1 \in I_1 \cap I_2 = \{0\},$$

thus $a_1 + a_2 = a_2 + a_1$ and $a_1 \circ a_2 = a_1 + a_2 = a_2 \circ a_1$. Hence

$$\begin{aligned} f((a_1 + a_2) \circ (b_1 + b_2)) &= f(a_1 \circ a_2 \circ b_1 \circ b_2) = f(a_1 \circ b_1 \circ a_2 \circ b_2) \\ &= f(a_1 \circ b_1 + a_2 \circ b_2) = (a_1 \circ b_1, a_2 \circ b_2) \\ &= (a_1, a_2) \circ (b_1, b_2) = f(a_1 + a_2) \circ f(b_1 + b_2), \end{aligned}$$

for all $a_1, b_1 \in I_1$ and $a_2, b_2 \in I_2$. □

thm:direct

Theorem 12.28. *Let n be a positive integer. Let A be a brace such that the additive group is a direct sum of ideals $I_1, \dots, I_n$, that is every element $a \in A$ is uniquely written as $a = a_1 + \cdots + a_n$, with $a_j \in I_j$ for all j. Then the map*

$$f : A \to I_1 \times \cdots \times I_n, \quad f(a_1 + \cdots + a_n) = (a_1, \dots, a_n),$$

for all $a_j \in I_j$, is an isomorphism of braces.

Proof. We shall prove the result by induction on n. For $n = 1$, it is clear. Suppose that $n > 1$ and that the result is true for $n - 1$. Let $A_1 = I_1 + \cdots + I_{n-1}$. Then A_1 is an ideal of A and A is the direct sum of the ideals A_1 and I_n. By Lemma 12.27, the map $f_1 : A \to A_1 \times I_n$ defined by $f(a + a_n) = (a, a_n)$, for all $a \in A_1$ and $a_n \in I_n$, is an isomorphism of braces. By the induction hypothesis, the map

$$f_2 : A_1 \to I_1 \times \cdots \times I_{n-1}, \quad f_2(a_1 + \cdots + a_{n-1}) = (a_1, \dots, a_{n-1}),$$

is an isomorphism of braces. Therefore $f = (f_2 \times \mathrm{id}) \circ f_1 : A \to I_1 \times \cdots \times I_n$ is an isomorphism of braces and $f(a_1 + \cdots + a_n) = (a_1, \dots, a_n)$, for all $a_j \in I_j$. The result then follows. □

cor:product

Corollary 12.29. *Let A be a finite brace such that $(A, +)$ and $(A, \circ)$ are nilpotent. Let $I_1, \dots, I_n$ be the distinct Sylow subgroups of the additive group of A. Then $I_1, \dots, I_n$ are ideals of A and the map*

$$f : A \to I_1 \times \cdots \times I_n, \quad f(a_1 + \cdots + a_n) = (a_1, \dots, a_n),$$

for all $a_j \in I_j$, is an isomorphism of braces.

Proof. Since $(A, +)$ is nilpotent, for every prime divisor p of the order of A, there is a unique Sylow p-subgroup I of $(A, +)$. Hence I is a normal subgroup of $(A, +)$, and $\lambda_a(b) \in I$ for all $a \in A$ and $b \in B$. Thus I is a left ideal of A and thus it is a Sylow p-subgroup of $(A, \circ)$. Since $(A, \circ)$ is nilpotent, I is the unique Sylow p-subgroup of $(A, \circ)$ and, thus, it is normal in $(A, \circ)$. Therefore I is an ideal of A. Hence $I_1, \dots, I_n$ are ideals of A and clearly the additive group of A is the direct sum of $I_1, \dots, I_n$. The result follows by Theorem 12.28. □

Let A be a brace. Let G be the multiplicative group of A and K be the additive group of A. The group G acts on K by automorphisms. Let G be the semidirect product $\Gamma = K \rtimes G$. The operation of G is

$$(x,g)(y,h) = (x + \lambda_g(y), g \circ h).$$

Identifying each $g \in G$ with $(0,g) \in \Gamma$ and each $x \in K$ with $(x,0) \in \Gamma$,

$$\begin{aligned}[g,x] &= gxg^{-1}x^{-1} = (0,g)(x,0)(0,g')(-x,0)\\ &= (\lambda_g(x),g)(-\lambda_g^{-1}(x),g') = (\lambda_g(x)-x,0) = \lambda_g(x)-x = g*x.\end{aligned}$$

Let $K_0 = K = A^1$ and $K_{n+1} = [G,K_n] = A^{n+2}$ for $n \geq 0$. The elements of the left series of A are iterated commutators of the group Γ.

pro:pgroups

Proposition 12.30. *Let p be a prime and A be brace of size p^m. Then A is left nilpotent.*

Proof. Let G be the multiplicative group of A and K be the additive group of A. Since the semidirect product $\Gamma = K \rtimes G$ is a p-group, it is nilpotent. Thus there exists k such that the k-repeated commutator $[\Gamma,\Gamma,\dots,\Gamma]$, where Γ appears k-times, is trivial. Since $A^k = [G,\dots,G,K] \subseteq [\Gamma,\dots,\Gamma]$, it follows that A is left nilpotent. □

Exercise 12.31. Let A be finite brace such that $A^3 = 0$. Then A^2 is a trivial brace of abelian type.

thm:A2

Theorem 12.32. *Let A be a finite left nilpotent brace. Then the following statements hold:*

1) *The additive group of A^2 is nilpotent.*
2) *The multiplicative group of $A/\ker\lambda$ is nilpotent.*

Proof. Since each element of the left series of A is a repeated commutator, the first claim follows from Hall's theorem [**?**, Theorem 4]. To prove the second claim, we use the notation above Proposition 12.30. Let $K = [G,X]G \subseteq \Gamma$ and $H = [G,X]X$. Let C be the centralizer of H in K. Then by [**?**, Theorem 4], K/C is locally nilpotent. Note that, since X is normal in Γ, $H = X$. Hence $G \cap C$ is the centralizer of X in G, that is

$$\begin{aligned}G \cap C &= \{g \in G \mid gxg^{-1} = x, \text{ for all } x \in X\}\\ &= \{g \in A \mid \lambda_g(x) = x, \text{ for all } x \in A\} = \ker\lambda.\end{aligned}$$

Thus $(GC)/C \cong G/(G \cap C) = G/\ker\lambda$ is locally nilpotent. □

The assumption on the nilpotency of the additive group in Theorem **??** is needed (see Example **??**).

Corollary 12.33. *Let A be a finite brace of size p^n for some prime number p and some positive integer n. Then either A is the trivial brace of order p or it is not simple.*

Proof. By Theorem **??**, A is left nilpotent. In particular, if $A \neq 0$, then $A^2 \neq A$. Since A^2 is an ideal either A is not simple or $A^2 = 0$. Assume that $A^2 = 0$. In this case, $a \circ b = a + b$ for all $a, b \in A$. Therefore $[A,A]$ is a proper an ideal of A. Hence, either A is not simple or $[A,A] = 0$. Assume that $A^2 = [A,A] = 0$. In this case A is a trivial brace and the result follows. □

lem:sylow_leftideals

Lemma 12.34. *Let A be a finite skew left brace with nilpotent additive group. Let p and q distinct prime numbers and let P and Q be Sylow subgroups of $(A,+)$ of sizes p^n and q^m, respectively. Then P, Q and $P+Q$ are left ideals of A.*

Proof. Let us first prove that P is a left ideal. Since $(A,+)$ is nilpotent, P is a normal subgroup of $(A,+)$. Let $a \in A$ and $x \in P$. Then $\lambda_a(x) \in P$ since λ_a is a group homomorphism. Similarly one proves that Q is a left ideal. From this it follows that $P+Q$ is a left ideal. □

The following is based on [61, Theorem 5(1)]. However, the proof is completely different.

thm:P*Q=0

Theorem 12.35. *Let A be a finite skew left brace with nilpotent additive group. Let p and q distinct prime numbers and let A_p and A_q be Sylow subgroups of $(A,+)$ of sizes p^n and q^m, respectively. If p does not divide $q^t - 1$ for all $t \in \{1,\dots,m\}$, then $A_p * A_q = 0$. In particular, $\lambda_x(y) = y$ for all $x \in A_p$ and $y \in A_q$.*

Proof. By Lemma 12.34 A_p, A_q and $A_p + A_q$ are left ideals of A. In particular, $A_p + A_q$ is a skew subbrace of A and A_p and A_q are Sylow subgroups of $(A_p + A_q, \circ)$. By Sylow's theorem, the number n_p of Sylow p-subgroups of the multiplicative group of $A_p + A_q$ is

$$n_p = [A_p + A_q : N] \equiv 1 \bmod p,$$

where $N = \{g \in A_p + A_q : g \circ A_p \circ g' = A_p\}$ is the normalizer of A_p in the multiplicative group of $A_p + A_q$. Since $[A_p + A_q : N] = q^s$ for some $s \in \{0,\dots,m\}$ and p does not divide $q^t - 1$ for all $t \in \{1,\dots,n\}$, it follows that $s = 0$ and hence A_p is a normal subgroup of the multiplicative group of $A_p + A_q$. Thus A_p is an ideal of the skew left brace $A_p + A_q$. Since A_p is an ideal of $A_p + A_q$ and A_q is a left ideal, we have that $A_p * A_q \subseteq A_p \cap A_q = 0$, and the result follows. □

Corollary 12.36. *Let A be a skew left brace of size $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, where $p_1 < p_2 < \cdots < p_k$ are prime numbers and $\alpha_1, \dots, \alpha_k$ are positive integers. Assume that the additive group of A is nilpotent. Let A_j be the Sylow p_j- subgroups of the additive group of A. Assume that, for some $j \leq k$, p_j does not divide $p_i^{t_i} - 1$ for all $t_i \in \{1, \dots \alpha_i\}$ for all $i \neq j$. Then $\operatorname{Soc}(A_j) \subseteq \operatorname{Soc}(A)$.*

Proof. Write $A = A_1 + \cdots + A_k$. Let $a \in \operatorname{Soc}(A_j)$ and $b \in A$. Hence there exist elements $b_k \in A_k$ such that $b = b_1 + \cdots + b_k$. By Theorem 12.35, $\lambda_a(b_i) = b_i$, for all $i \neq j$. Then $\lambda_a(b) = \lambda_a(b_1) + \cdots + \lambda_a(b_k) = b_1 + \cdots + b_k = b$ and hence $a \in Soc(A)$. Thus the result follows. □

Let A be a skew left brace. For subsets X and Y of A we define inductively $L_0(X,Y) = Y$ and $L_{n+1}(X,Y) = X * L_n(X,Y)$ for $n \geq 0$.

Definition 12.37. Let p be a prime number. A finite skew left brace A of nilpotent type is said to be *left p-nilpotent* if there exists $n \geq 1$ such that $L_n(A, A_p) = 0$, where A_p is the Sylow p-subgroup of $(A, +)$.

lem:factorization **Lemma 12.38.** *Let A be a skew left brace such that its additive group is the direct product of the left ideals B and C. Then $A * (B + C) = A * B + A * C$. Moreover, if $A = \oplus_{i=1}^{n} B_i$ where the B_i are left ideals, then*

$$A * \sum_{i=1}^{n} B_i = \sum_{i=1}^{n} A * B_i.$$

Proof. Let $a \in A$, $b \in B$ and $c \in C$. Then

$$a * (b + c) = a * b + b + a * c - b = a * b + a * c$$

holds for all $a \in A$, $b \in B$ and $c \in C$. The second part follows by induction. □

pro:left_p **Proposition 12.39.** *Let A be a finite skew left brace of nilpotent type. Then A is left nilpotent if and only if A is left p-nilpotent for all $p \in \pi(A)$.*

Proof. For each $p \in \pi(A)$ there exists $n(p) \in \mathbb{N}$ such that $L_{n(p)}(A, A_p) = \{0\}$. Let $n = \max\{n(p) : p \in \pi(A)\}$. Then $L_n(A, A_p) = \{0\}$ for all $p \in \pi(A)$. Since A is of nilpotent type, the additive group $(A, +)$ is isomorphic to the direct sum of the A_p for $p \in \pi(A)$. Then Lemma 12.38 implies that

$$L_n(A, A) = \sum_{p \in \pi(A)} L_n(A, A_p) = \{0\}.$$

The other implication is trivial. □

We now recall some notation about commutators. Given a brace A, the group $(A, \circ)$ acts on $(A, +)$ by automorphisms. If in the semidirect product $(A, +) \rtimes (A, \circ)$ we identify a with $(0, a)$ and b with $(b, 0)$, then

$$\begin{aligned} [a, b] &= (0, a)(b, 0)(0, a)^{-1}(b, 0)^{-1} = (0, a)(b, 0)(0, a')(-b, 0) \\ &= (\lambda_a(b), a)(-\lambda_{a'}(b), a') = (\lambda_a(b) - b, 0) \\ &= (a * b, 0) \end{aligned}$$

Under this identification, we write $[X, Y] = X * Y$ for any pair of subsets $X, Y \subseteq A$. Then the iterated commutator satisfies

$$[X, \dots, X, Y] = [X, [X, \dots, [X, Y] \dots]] = L_n(X, Y),$$

where the subset X appears n times.

thm:left_p **Theorem 12.40.** *Let A be a finite brace of nilpotent type. The following statements are equivalent:*

1) *A is left p-nilpotent.*

2) $A_{p'} * A_p = \{0\}$.
3) *The group* $(A,\circ)$ *is* p*-nilpotent.*

Proof. We first prove that (1) implies (2). Since A is left p-nilpotent, there exists $n \in \mathbb{N}$ such that $L_n(A_{p'},A_p) \subseteq L_n(A,A_p) = \{0\}$. Since $(A_{p'},\circ)$ acts by automorphisms on $(A_p,+)$ and this is a coprime action, it follows from [39, Lemma 4.29] that

$$L_1(A_{p'},A_p) = A_{p'} * A_p = A_{p'} * (A_{p'} * A_p) = L_2(A_{p'},A_p).$$

By induction one then proves that $A_{p'} * A_p = L_n(A_{p'},A_p) = \{0\}$.

We now prove that (2) implies (3). It is enough to prove that $(A_{p'},\circ)$ is a normal subgroup of $(A,\circ)$. By using Lemma 12.38,

$$A_{p'} * A = A_{p'} * (A_p + A_{p'}) = (A_{p'} * A_p) + (A_{p'} * A_{p'}) \subseteq A_{p'}.$$

since A'_p is a left ideal of A and $A_{p'} * A_p = \{0\}$. Then $A_{p'}$ is an ideal of A by Lemma **??** and [**?**, Lemma 1.9]. In particular, $(A_{p'},\circ)$ is a normal subgroup of $(A,\circ)$.

Finally we prove that (3) implies (1). We need to prove that $L_n(A_p,A_p) = 0$ for some n. Since $(A,\circ)$ is p-nilpotent, there exists a normal p-complement that is a characteristic subgroup of $(A,\circ)$. This group is $A_{p'}$ and hence $A_{p'}$ is an ideal of A. Then $A_{p'} * A_p \subseteq A_{p'} \cap A_p = 0$. We now prove that $L_n(A,A_p) = L_n(A_p,A_p)$ for all $n \geq 0$. The case where $n = 0$ is trivial, so assume that the result holds for some $n \geq 0$. By the inductive hypothesis,

$$L_{n+1}(A,A_p) = A * L_n(A,A_p) = A * L_n(A_p,A_p).$$

Thus it is enough to prove that $A * L_n(A_p,A_p) \subseteq A_p * L_n(A_p,A_p)$. Let $a \in A$ and $b \in L_n(A_p,A_p)$. Write $a = x \circ y$ for $x \in A_p$ and $y \in A_{p'}$. Then

$$a * b = (x \circ y) * b = x * (y * b) + y * b + x * b = x * b \in A_p * L_n(A_p,A_p)$$

since $A_{p'} * A_p = 0$. The skew left brace A_p is left nilpotent by [**?**, Proposition 4.4], so there exists $n \in \mathbb{N}$ such that $L_n(A_p,A_p) = 0$. $\square$

Exercises

prob:LN_direct

12.1. Let $A_1,\dots,A_k$ be left nilpotent braces. Prove that $A_1 \times \cdots \times A_k$ is left nilpotent.

prob:LN_surj

12.2. Let $f\colon A \to B$ be a surjective homomorphism of braces. Prove that if A is left nilpotent, then B is left nilpotent.

prob:LN_sub

12.3. Let A be a left nilpotent brace and $B \subseteq A$ be a sub brace. Prove that B is left nilpotent.

prob:nil=>leftnilpotent

12.4. Prove that nil braces of abelian/nilpotent type? left nilpotent.

Open problems

tion:rightnil=>rightnilp **Open problem 12.1.** Let A be a finite right nil brace. Is A right nilpotent?

tronglynil=>stronglynilp **Open problem 12.2.** Let A be a finite strongly nil brace. Is A strongly nilpotent?

Notes

The left series of a brace was defined by Rump [56] in the context of braces of abelian type. Precisely in that paper he proved Proposition 12.30 by a different method in the case of braces of abelian type.

Strongly nilpotent braces of abelian type were defined by Smoktunowicz in [62]. These definitions extend to skew left braces, see [22].

Theorem 12.28 was proved by Byott in the context of Hopf–Galois extensions [14].

Theorem **??** was proved by Smoktunowicz in [62] for braces of abelian type and it was extended to nilpotent type in [22].

Theorem **??** was proved By Smoktunowicz in [62, Theorem 1.1] for braces of abelian type. The generalization to braces of nilpotent type appeared in [22, Theorem 4.8]. The proof presented in this chapter appeared in [1] and it is heavily based on the ideas of Ballester–Bolinches, Meng and Romero [49].

Theorem 12.40 was proved by Ballester–Bolinches, Meng and Romero for braces of abelian type.

Exercise 12.4 was proved in the case of braces of abelian type by Smoktunowicz [61].

Chapter 13
Multipermutation solutions

MP

A

If X is a solution, we consider over X the relation

$$x \sim y \iff \sigma_x = \sigma_y \text{ and } \tau_x = \tau_y.$$

Then $\sim$ is an equivalence relation. Let $\overline{X}$ be the set of equivalence classes and $[x]$ denote the equivalence class of x.

Proposition 13.1. *Let (X,r) be a solution. Then $(\overline{X},\overline{r})$, where*

$$\overline{r}([x],[y]) = ([\sigma_x(y)],[\tau_y(x)]),$$

is a solution.

Proof. We first prove that $\overline{r}$ is well-defined. Let $x,y \in X$ be such that $x \sim y$ and let $z \in X$. Since (X,r) is a solution, Lemma 1.3 implies that

$$\sigma_{\sigma_x(z)} \circ \sigma_{\sigma_z(x)} = \sigma_x \circ \sigma_z = \sigma_y \circ \sigma_z = \sigma_{\sigma_y(z)} \circ \sigma_{\sigma_z(x)},$$

it follows that $\sigma_{\sigma_z(x)} = \sigma_{\sigma_z(y)}$ and hence $\sigma_z(x) \sim \sigma_z(y)$. Similarly $\tau_{\tau_z(x)} = \tau_{\tau_z(y)}$ and therefore $\overline{r}$ is well-defined.

We now prove that $\overline{r}$ is invertible.

... $\square$

In the case of involutive solutions, it follows from Proposition 2.56 that $\sigma_x = \sigma_y$ if and only if $\tau_x = \tau_y$.

Definition 13.2. Let (X,r) be a solution. The solution $\operatorname{Ret}(X,r) = (\overline{X},\overline{r})$ induced by the equivalence relation $\sim$ is the *retraction* of (X,r).

We define inductively $\operatorname{Ret}^0(X,r) = (X,r)$, $\operatorname{Ret}^1(X,r) = \operatorname{Ret}(X,r)$ and

$$\operatorname{Ret}^{n+1}(X,r) = \operatorname{Ret}(\operatorname{Ret}^n(X,r)) \quad n \geq 1.$$

Definition 13.3. A solution (X,r) is said to be of *multipermutation level n* if n is the smallest non-negative integer such that $|\mathrm{Ret}^n(X,r)|=1$. The solution (X,r) is said to be *irretractable* if $\mathrm{Ret}(X,r)=(X,r)$.

The trivial solution over the set with one element is a multipermutation of level zero. Permutation solutions are multipermutation solutions of level one.

Example 13.4.

Example 13.5.

Table 13.1: Involutive solutions of size ≤ 10.

tab:INV_mp

n	2	3	4	5	6	7	8	9	10
solutions	2	5	23	88	595	3456	34530	321931	4895272
multipermutation	2	5	21	84	554	3295	32155	305916	4606440
irretractable	0	0	2	4	9	13	191	685	3590

For size ≤ 7 the numbers of Table 13.1 coincide with those in [32] but there are some differences for solutions of size eight.

Table 13.2: Non-involutive solutions of size ≤ 8.

tab:mp

n	2	3	4	5	6	7	8
solutions	2	21	230	3519	100071	4602720	422449480
multipermutation		15	206	3165	95517	4461805	416725250
irretractable		6	24	98	514	2659	17370

thm:CJKAV

Theorem 13.6. *Let (X,r) be a finite multipermutation solution. If $|X|>1$, then r has even order.*

Proof. Since $(X,r)\to\mathrm{Ret}(X,r)$, $x\mapsto[x]$ is a homomorphism of solutions, it follows that the order of the solution $\bar{r}$ divides de orden of r. Assume that (X,r) has multipermutation level n. There exists a homomorphism of solutions $(X,r)\to\mathrm{Ret}^{n-1}(X,r)$, thus it is enough to prove the theorem in the case where $r(x,y)=(\sigma(y),\tau(x))$ for commuting permutations σ and τ, i.e. multipermutation solutions of level one. If r has order $2k+1$, then

$$(x,y)=r^{2k+1}(x,y)=(\sigma^{k+1}\tau^k(y),\sigma^k\tau^{k+1}(x)).$$

This implies that $\sigma^{k+1}\tau^k(y)=x$ for all $x,y\in X$. This equality in particular implies that $x=y$ because $\sigma^{k+1}\tau^k$ is a permutation, a contradiction. $\square$

The connection between the socle of a brace and the retract of a solution was discovered by Rump in the case of involutive solutions and braces of abelian type, see [56].

pro:add_cyclic

Proposition 13.7. *Let A be a brace and (A,r) be its associated solution. Then the retraction* $\operatorname{Ret}(A,r)$ *is the canonical solution associated with the quotient brace* $A/\operatorname{Soc}(A)$.

Proof. The equivalence relation $\sim$ on A is defined as $a \sim b$ if and only if $\lambda_a = \lambda_b$ and $\mu_a = \mu_b$. Let $\overline{A}$ be the set of equivalence classes. The equivalence class of an element a is then

$$\begin{aligned}[a] &= \{b \in A : a \sim b\} = \{b \in A : \lambda_a = \lambda_b,\, \mu_a = \mu_b\}\\ &= \{b \in A : a' \circ b \in \ker\lambda \cap \ker\mu\} = \{b \in A : a' \circ b \in \operatorname{Soc}(A)\},\end{aligned}$$

by Proposition 4.37. This means that $[a] = [b]$ if and only if $\pi(a) = \pi(b)$, where $\pi\colon A \to A/\operatorname{Soc}(A)$, $x \mapsto x \circ \operatorname{Soc}(A)$, is the canonical brace homomorphism. Moreover, $A/\operatorname{Soc}(A) = \overline{A}$ as sets. Now we compute the retraction of (A,r):

$$\begin{aligned}\overline{r}([a],[b]) &= ([\lambda_a(b)],[\mu_b(a)]) = (\pi(\lambda_a(b)),\pi(\mu_b(a)))\\ &= \left(\lambda_{\pi(a)}(\pi(b)),\mu_{\pi(b)}(\pi(a))\right) = \left(\lambda_{[a]}([b]),\mu_{[b]}([a])\right).\end{aligned}$$

Therefore $\operatorname{Ret}(A,r) = (A/\operatorname{Soc}(A),\overline{r})$. ☐

Now...

pro:mpl

Proposition 13.8. *Let (X,r) and (Y,s) be solutions. Each surjective homomorphism of solutions $f\colon (X,r) \to (Y,s)$ induces a surjective homomorphism of solutions* $\operatorname{Ret}(X,r) \to \operatorname{Ret}(Y,s)$.

Proof. Write $r(x,y) = (\sigma_x(y),\tau_y(x))$ and $s(x,y) = (\lambda_x(y),\mu_y(x))$. Let $x, x_1 \in X$ be such that $x \sim x_1$. If $z \in X$, then

$$\lambda_{f(x)}f(z) = f(\sigma_x(z)) = f(\sigma_{x_1}(z)) = \lambda_{f(x_1)}f(z).$$

Since f is surjective, it follows that $\lambda_{f(x)} = \lambda_{f(x_1)}$. A similar calculation proves that $\mu_{f(x)} = \mu_{f(x_1)}$. If $\pi\colon (Y,s) \to \operatorname{Ret}(Y,r)$, $y \mapsto [y]$, is the canonical map, the composition $\pi \circ f\colon (X,r) \to \operatorname{Ret}(Y,s)$ is a surjective homomorphism of solutions. Therefore the map $\operatorname{Ret}(X,r) \to \operatorname{Ret}(Y,s)$, $[x] \mapsto \pi(f(x))$, is then a well-defined surjective homomorphism of solutions. ☐

pro:mpl_subsol

Proposition 13.9. *Let (X,r) be a solution of finite multipermutation level m and $Y \subseteq X$ be such that $r(Y \times Y) \subseteq Y \times Y$. Then the* subsolution $(Y, r|_{Y\times Y})$ *is of finite multipermutation level $\leq m$.*

Proof. ☐

Theorem 13.10. *Let (X,r) be a solution. The following statements are equivalent:*

1) *(X,r) has finite multipermutation level.*
2) *$\left(\mathcal{G}(X,r), r_{\mathcal{G}(X,r)}\right)$ has finite multipermutation level.*
3) *$\left(G(X,r), r_{G(X,r)}\right)$ has finite multipermutation level.*

Proof. Let us first prove that (2) implies (1). The map $X \to \mathscr{G}(X,r)$, $x \mapsto (\lambda_x, \mu_x^{-1})$, is a homomorphism of solutions that induces an injective homomorphism of solutions $\operatorname{Ret}(X,r) \to \left(\mathscr{G}(X,r), r_{\mathscr{G}(X,r)}\right)$. Since $\left(\mathscr{G}(X,r), r_{\mathscr{G}(X,r)}\right)$ has finite multipermutation level, (X,r) has finite multipermutation level by Proposition 13.9.

Let us now prove that (3) implies (2). The canonical map $G(X,r) \to \mathscr{G}(X,r)$ yields a surjective homomorphism of solutions. Then Proposition 13.8 applies.

... □

The following result appeared in [32].

Proposition 13.11. *Let (X,r) be a finite involutive solution. If the additive group of the brace $\mathscr{G}(X,r)$ is cyclic, then (X,r) is multipermutation.*

Proof. Let (X,r) be a counterexample of minimal cardinality. If K is the additive group of $\mathscr{G}(X,r)$, then K is finite and cyclic. Write G for the multiplicative group of $\mathscr{G}(X,r)$. Since $|\operatorname{Aut}(K)| = \varphi(|K|) < |K|$, where φ is the Euler function, the group homomorphism $\lambda\colon G \to \operatorname{Aut}(K)$ has a non-trivial kernel, so $\operatorname{Soc}(\mathscr{G}(X,r))$ is non-zero. This implies that (X,r) is retractable. Since $\mathscr{G}(X,r)/\operatorname{Soc}(\mathscr{G}(X,r))$ is a brace with cyclic additive group and $\operatorname{Ret}(X,r)$ is an involutive solution, the minimality of $|X|$ implies that $\operatorname{Ret}(X,r)$ is a multipermutation solution, and hence so is (X,r), a contradiction. □

The converse of the previous proposition does not hold.

Example 13.12. Let $X = \{1,2,3,4\}$ and $r(x,y) = (\varphi_x(y), \varphi_y(x))$, where

$$\varphi_1 = \varphi_2 = \mathrm{id}, \quad \varphi_3 = (34), \quad \varphi_4 = (12)(34).$$

Then (X,r) is an involutive multipermutation solution. One easily checks that $\mathscr{G}(X,r) \simeq C_2 \times C_2$.

A similar idea proves the following result:

thm:mul_cyclic **Theorem 13.13.** *Let (X,r) be a finite involutive solution. If the multiplicative group of the brace $\mathscr{G}(X,r)$ is cyclic, then (X,r) is multipermutation.*

Proof. Let (X,r) be a counterexample of minimal cardinality. Write K for the additive group of $\mathscr{G}(X,r)$ and $G = \langle g \rangle$ for the multiplicative group of $\mathscr{G}(X,r)$. Since the image of the group homomorphism $\lambda\colon G \to \operatorname{Aut}(K)$ is cyclic generated by λ_g and $|\lambda_g| < |G|$ by Horosevskii's theorem, see [39, Corollary 3.3], it follows that λ has a non-trivial kernel, so $\operatorname{Soc}(\mathscr{G}(X,r))$ is non-zero. This implies that (X,r) is retractable. Since $\mathscr{G}(X,r)/\operatorname{Soc}(\mathscr{G}(X,r))$ is a brace with cyclic additive group and $\operatorname{Ret}(X,r)$ is an involutive solution, the minimality of $|X|$ implies that $\operatorname{Ret}(X,r)$ is a multipermutation solution, and hence so is (X,r), a contradiction. □

The previous result does not hold in the case of arbitrary solutions.

Example 13.14. Let $X = \{1,2,3,4,5,6\}$ and $r(x,y) = (\sigma_x(y), \tau_y(x))$, where

$$\begin{array}{lll}
\sigma_1 = \mathrm{id}, & \sigma_2 = \mathrm{id}, & \sigma_3 = \mathrm{id}, \\
\sigma_4 = (23)(56), & \sigma_5 = (23)(56), & \sigma_6 = (23)(56), \\
\tau_1 = \mathrm{id}, & \tau_2 = (456), & \tau_3 = (465), \\
\tau_4 = \mathrm{id}, & \tau_5 = (465), & \tau_6 = (456).
\end{array}$$

The brace $\mathscr{G}(X,r)$ has multiplicative group isomorphic to $\mathbb{S}_3$ and additive group isomorphic to the cyclic group of order six.

We will see later that Theorem 13.13 is true for braces of nilpotent type. The following example appears in the work of Rump [56].

pro:radical **Proposition 13.15.** *Let A be a finite non-trivial radical ring. Then* $\mathrm{Soc}(A) \neq \{0\}$ *and (A, r_A) is an involutive multipermutation solution.*

Proof. Let A be a counterexample of minimal size. This means that $\mathrm{Soc}(A) = \{0\}$ and all two-sided braces of abelian type of size $< |A|$ have non-trivial socle. Since A is finite, there exists a non-zero minimal left ideal I of A. Recall that A is a radical ring with product $a * b = \lambda_a(b) - b$. Since A is a radical ring, A is a nil ring, which implies by Nakayama's lemma that $I * A = \{0\}$. This means that if $x \in I$, then $x \in \mathrm{Soc}(A)$, as $0 = x * a = \lambda_x(a) - a$ for all $a \in A$. In particular, $\mathrm{Soc}(A) \neq \{0\}$, a contradiction. $\square$

Proposition 13.15 has a nice application. The results appeared first in [20]. The proof presented here is from [21].

thm:CJO_abelian **Theorem 13.16.** *Let (X,r) be a finite involutive solution. If the multiplicative group of the brace $\mathscr{G}(X,r)$ is abelian, then (X,r) is multipermutation.*

Proof. $\square$

In [34], Gateva–Ivanova conjectured that finite involutive square-free solutions are retractable.

In [35] Gateva–Ivanova asked when...

Right nilpotency...

The following theorem characterizes multipermutation involutive solutions in terms of left orderability of groups. A group G is said to be *left ordered* if it admits a total ordering $<$ such that

$$x < y \implies zx < zy$$

for all $x,y,z \in G$. Torsion-free abelian groups, free groups and braid groups are left ordered groups. See [26] for more information on ordered groups.

thm:BCV **Theorem 13.17.** *Let (X,r) be a finite involutive solution. The following statements are equivalent:*

1) *(X,r) is a multipermutation solution.*
2) *$G(X,r)$ is poly-$\mathbb{Z}$.*
3) *$G(X,r)$ is left orderable.*
4) *$G(X,r)$ is diffuse.*

Proof. □

Recall that a group G has the *unique product property* if for all finite non-empty subsets A and B of G there exists $x \in G$ that can be written uniquely as $x = ab$ with $a \in A$ and $b \in B$.

It is natural to ask when $G(X,r)$ has the unique product property. By Theorem 13.17, if (X,r) is an involutive multipermutation solution, then $G(X,r)$ has the unique product property since $G(X,r)$ is left orderable.

pro:4-19 **Example 13.18.** Let $X = \{1,2,3,4\}$ and $r(x,y) = (\sigma_x(y), \tau_y(x))$ be the irretractable involutive solution given by

$$\begin{aligned} &\sigma_1 = (12), && \sigma_2 = (1324), && \sigma_3 = (34), && \sigma_4 = (1423),\\ &\tau_1 = (14), && \tau_2 = (1243), && \tau_3 = (23), && \tau_4 = (1342). \end{aligned}$$

We claim that the group $G(X,r)$ with generators x_1,x_2,x_3,x_4 and relations

$$\begin{aligned} &x_1^2 = x_2x_4, && x_1x_3 = x_3x_1, && x_1x_4 = x_4x_3,\\ &x_2x_1 = x_3x_2, && x_2^2 = x_4^2, && x_3^2 = x_4x_2. \end{aligned}$$

does not have the unique product property. Let $x = x_1x_2^{-1}$ and $y = x_1x_3^{-1}$ and

$$\begin{aligned} S = \{&x^2y, y^2x, xyx^{-1}, (y^2x)^{-1}, (xy)^{-2}, y, (xy)^2x, (xy)^2,\\ &(xyx)^{-1}, yxy, y^{-1}, x, xyx, x^{-1}\}. \end{aligned} \tag{13.1}$$ eq:Promislow

To prove that $G(X,r)$ does not have the unique product property it is enough to prove that each $s \in S^2 = \{s_1s_2 : s_1,s_2 \in S\}$ admits at least two different decompositions of the form $s = ab = uv$ for $a,b,u,v \in S$. To perform these calculations we use the injective group homomorphism $G \to \mathbf{GL}(5,\mathbb{Z})$ given by

$$x_1 \mapsto \begin{pmatrix} 0&1&0&0&1\\ 1&0&0&0&0\\ 0&0&1&0&0\\ 0&0&0&1&0\\ 0&0&0&0&1 \end{pmatrix}, \qquad x_2 \mapsto \begin{pmatrix} 0&0&0&1&0\\ 0&0&1&0&1\\ 1&0&0&0&0\\ 0&1&0&0&0\\ 0&0&0&0&1 \end{pmatrix},$$
$$x_3 \mapsto \begin{pmatrix} 1&0&0&0&0\\ 0&1&0&0&0\\ 0&0&0&1&1\\ 0&0&1&0&0\\ 0&0&0&0&1 \end{pmatrix}, \qquad x_4 \mapsto \begin{pmatrix} 0&0&1&0&0\\ 0&0&0&1&0\\ 0&1&0&0&0\\ 1&0&0&0&1\\ 0&0&0&0&1 \end{pmatrix}.$$

This faithful representation of $G(X,r)$ allows us to compute all possible products of the form s_1s_2 for all $s_1,s_2 \in S$. By inspection, each element of S^2 admits at least two different representations.

thm:CJO_mp **Theorem 13.19.** *Let A be a finite brace of abelian type with multiplicative group G. Then there exists a finite solution (X,r) such that* $\operatorname{Ret}(X,r)$ *is isomorphic to (A,r_A) and $\mathscr{G}(X,r)\simeq G$.*

Proof. Let $X=A\times\mathbb{Z}/(2)$. For $a,b\in A$, let

$$\varphi_{(a,0)}(b,0)=(b,0),\qquad \varphi_{(a,0)}(b,1)=(b,1),$$
$$\varphi_{(a,1)}(b,0)=(a'\circ b,0),\qquad \varphi_{(a,1)}(b,1)=(\lambda_a^{-1}(b),1).$$

The maps $\varphi_{(a,\varepsilon)}$ are invertible for all $a\in A$ and $\varepsilon\in\mathbb{Z}/(2)$. In fact,

$$\varphi_{(a,0)}^{-1}=\mathrm{id},\quad \varphi_{(a,1)}^{-1}(b,\varepsilon)=\begin{cases}a\circ b & \text{if } \varepsilon=0,\\ \lambda_a(b) & \text{if } \varepsilon=1.\end{cases}$$

So we need to check that

$$((a,\varepsilon_1)\cdot(b,\varepsilon_2))\cdot((a,\varepsilon_1)\cdot(c,\varepsilon_3))=((b,\varepsilon_2)\cdot(a,\varepsilon_1))\cdot((b,\varepsilon_2)\cdot(c,\varepsilon_3))\tag{13.2}$$ eq:CJO_tocheck

holds for all $a,b,c\in A$ and $\varepsilon_1,\varepsilon_2,\varepsilon_3\in\mathbb{Z}/(2)$. There are several cases to consider. Let us assume first that $(\varepsilon_1,\varepsilon_2,\varepsilon_3)=(1,1,0)$. Then (13.2) turns out to be

$$(\lambda_a^{-1}(b)'\circ a'\circ c,0)=(\lambda_b^{-1}(a)'\circ b'\circ c,0),$$

which holds for all $a,b\in A$, as

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

because A is of abelian type. Let us now deal with the case $(\varepsilon_1,\varepsilon_2,\varepsilon_3)=(1,1,1)$. In this case Equality (13.2) turns out to be equivalent to

$$(\lambda_a^{-1}(b),1)\cdot(\lambda_a^{-1}(c),1)=(\lambda_b^{-1}(a),1)\cdot(\lambda_b^{-1}(c),1).$$

Since A is of abelian type,

$$\begin{aligned}(\lambda_a^{-1}(b),1)\cdot(\lambda_a^{-1}(c),1)&=\lambda^{-1}_{\lambda_a^{-1}(b)}\lambda_a^{-1}(c)=\lambda^{-1}_{a\circ\lambda_a^{-1}(b)}(c)=\lambda^{-1}_{a+b}(c)\\ &=\lambda^{-1}_{b+a}(c)=\lambda^{-1}_{\lambda_b^{-1}(a)}\lambda_b^{-1}(c)=(\lambda_b^{-1}(a),1)\cdot(\lambda_b^{-1}(c),1).\end{aligned}$$

The other cases are easier and require straightforward calculations.

Let $\psi\colon G\to\mathbb{S}_X$, $\psi(g)=\varphi_{(g',1)}$. Since

$$\psi(g)(0,0)=\varphi_{(g',1)}(0,0)=(g\circ 0,0)=(g,0),$$

it follows that ψ is injective. Moreover, ψ is a group homomorphism, as

$$\begin{aligned}\psi(a)\psi(b)(c,0)&=\psi(a)\varphi_{(b,1)}(c,0)=\psi(a)(b\circ c,0)\\ &=\varphi_{(a,1)}(b\circ c,0)=(a\circ b\circ c,0)=\varphi_{(a\circ b,1)}(c,0)=\psi_{(a\circ b)}(c,0)\end{aligned}$$

and

$$\begin{aligned}\psi(a)\psi(b)(c,1) &= \varphi_{(a',1)}\varphi_{(b',1)}(c,1) = \varphi_{(a',1)}(\lambda_{b'}^{-1}(c),1)\\ &= (\lambda_{a'}^{-1}\lambda_{b'}^{-1}(c),1) = (\lambda_{a\circ b}(c),1) = \varphi_{(a\circ b,1)}(c,1) = \psi(a\circ b)(c,1).\end{aligned}$$

Since ψ is an injective group homomorphism,

$$G \simeq \psi(G) \simeq \langle \psi(a) : a \in A\rangle = \langle \varphi_{(a,1)} : a \in A\rangle \simeq \mathscr{G}(X,r).$$

Consider the equivalence relation on X given by $x \sim y$ if and only if $\varphi_x = \varphi_y$. As usual $[x]$ denotes the equivalence class of the element $x \in X$ and $\overline{X}$ is the set of equivalence classes. A straightforward computation shows that $(a,0) \sim (0,1)$ for all $a \in A$. This implies that

$$\overline{p}\colon \overline{X} \to A, \quad \overline{p}([(a,\varepsilon)]) = \begin{cases} 0 & \text{if } \varepsilon = 0,\\ a & \text{if } \varepsilon = 1,\end{cases}$$

is a well-defined surjective map. We claim that $\overline{p}$ is injective. Let $(a,\varepsilon_1) \in \overline{X}$ and $(b,\varepsilon_2) \in \overline{X}$ be such that $\overline{p}([(a,\varepsilon_1)]) = \overline{p}([(b,\varepsilon_2)])$. Since $[(a,0)] = [(0,1)]$ for all $a \in A$, we only need to consider the case where $\varepsilon_1 = \varepsilon_2 = 1$. In this case,

$$a = \overline{p}([(a,\varepsilon_1)]) = \overline{p}([(b,\varepsilon_2)]) = b.$$

Thus $\overline{p}$ is bijective. Now

$$\begin{aligned}r_A(\overline{p}[(a,1)],\overline{p}[(b,1)]) &= r_A(a,b) = (\lambda_a(b),\mu_b(a)) = (\overline{p}[\lambda_a(b),1],\overline{p}[\mu_b(a),1])\\ &= (\overline{p}\varphi_{(a,1)}(b,1),\overline{p}...).\end{aligned}$$

□

Theorem 13.20. *Let A be...*

Proof. □

Exercises

prob:bounded_mpl **13.1.** Let (X,r) be a solution of finite multipermutation level m. Prove that any homomorphic image of (X,r) is a solution of finite multipermutation level $\leq m$.

prob:4-13 **13.2.** Let $X = \{1,2,3,4\}$ and $r(x,y) = (\sigma_x(y),\tau_y(x))$ be the irretractable involutive solution given by

$$\begin{aligned}&\sigma_1 = (34), && \sigma_2 = (1324), && \sigma_3 = (1423), && \sigma_4 = (12),\\ &\tau_1 = (24), && \tau_2 = (1432), && \tau_3 = (1234), && \tau_4 = (13).\end{aligned}$$

Prove that $G(X,r)$ does not have the unique product property.

Open problems

Open problem 13.1. Does the group $G(X,r)$... A linear representation of this group is...

Notes

Multipermutation involutive solutions were introduced in [32]. The notion was extended to the non-involutive case in [47].

Theorem 13.6 was proved in...

Proposition 13.8 was proved in [21] for involutive solutions. The general case goes back to...

Theorem 13.17 combines several results. The implication...

Theorem 13.19 appears in [21].

Non-involutive multipermutation solutions...

The set (13.1) appears in the work of Promislow [53]. Exercise 13.2 appears in the book of Jespers and Okniński, see [43, Example 8.2.14].

Chapter 14
Ordered groups

ordered

A

A group G is **left-orderable** is there is a total ordering $<$ on G such that $x < y$ implies $zx < zy$ for all $x, y, z \in G$. Similarly one defines right ordered groups.

Example 14.1. The group $\mathbb{Z}$ is left-orderable.

Example 14.2. If G is a left-orderable group and H is a subgroup of G, then H is left-orderable.

Example 14.3. Let $G = \mathbb{Z}^2$ and $v \in \mathbb{R}^2$ with irrational slope. Then...

Proposition 14.4. *Let*

$$1 \longrightarrow K \xrightarrow{\iota} G \xrightarrow{p} Q \longrightarrow 1$$

be a short exact sequence of groups. If both K and Q are left-orderable, then G is left-orderable.

Proof. We define

$$x < y \Longleftrightarrow \begin{cases} 1 <_K x^{-1}y & \text{if } p(x) = p(y), \\ p(x) <_Q p(y) & \text{otherwise.} \end{cases}$$

A straightforward computation shows that then G is left-orderble. □

Example 14.5. Let us show that $G = \langle x, y : xyx^{-1} = y^{-1} \rangle$ is left-orderable. Let $f\colon G \to \mathbb{Z}$ be given by $x \mapsto 1$ and $y \mapsto 0$. Then $\ker f = \langle y \rangle$ and the sequence

$$1 \longrightarrow \langle y \rangle \longrightarrow G \longrightarrow \mathbb{Z} \longrightarrow 1$$

is exact. The map

$$G \to \mathbf{GL}_2(\mathbb{C}), \quad x \mapsto \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \quad y \mapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

is a group homomorphism. In particular, y has infinite order and hence $\langle y \rangle \simeq \mathbb{Z}$ is left orderable. The previous proposition implies then that G is left-orderable.

The previous example is the Baumslag–Solitar group $B(1,-1)$. Recall that for $n,m \in \mathbb{Z}$ the Baumslag–Solitar's group is defined as the group

$$B(m,n) = \langle a,b : ba^m b^{-1} = a^n \rangle.$$

The map

$$B(m,n) \to \mathbf{GL}_2(\mathbb{C}), \quad a \mapsto \begin{pmatrix} \frac{m}{n} & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad b \mapsto \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$$

is a group homomorphism.

A group G is said to be **poly-$\mathbb{Z}$** if...

Exercise 14.6. Prove that poly-$\mathbb{Z}$ groups are left-orderable.

A group G is said to be **indicable** if there exists a non-trivial group homomorphism $G \to \mathbb{Z}$, and G is said to be **locally indicable** if every finitely generated subgroup of G is indicable.

FIXME

Theorem 14.7 (Burns–Hale). *Let G be a group. Then G is left-orderable if and only if for each finitely generated non-trivial subgroup H of G there exists a left-ordered group L and a non-trivial group homomorphism $H \to L$.*

Proof. If G is left-orderable, take $L = H$.

Let L be a left-orderable group. We claim that for all $\{x_1,\dots,x_n\} \subseteq G \setminus \{1\}$ there exist $\varepsilon_1,\dots,\varepsilon_n \in \{-1,1\}$ such that

$$1 \notin S(x_1^{\varepsilon_1},\dots,x_n^{\varepsilon_n}),$$

where $S(x_1^{\varepsilon_1},\dots,x_n^{\varepsilon_n})$ denotes the semigroup generated by the set $\{x_1^{\varepsilon_1},\dots,x_n^{\varepsilon_n}\}$. We proceed by induction on n. If $n = 1$, then $x_1 \in G \setminus \{1\}$. Let $\varepsilon_1 = 1$. If $1 \in S(x_1)$, then x_1 is an element of finite order and hence $\langle x_1 \rangle \to L$ is the trivial homomorphism. Now assume that the claim holds for some $n \geq 1$. Let $\{x_1,\dots,x_n\} \subseteq G \setminus \{1\}$. By assumption, there exists a non-trivial group homomorphism $h\colon \langle x_1,\dots,x_n \rangle \to L$. In particular, $h(x_i) \neq 1$ for some $i \in \{1,\dots,n\}$. Without loss of generality we may assume that $h(x_j) \neq 1$ for all $j \in \{1,\dots,k-1\}$ and $h(j) = 1$ for all $j > k$. Since L is left-orderable and $h(x_j) \neq 1$ for all $j \leq k$, there are elements $\varepsilon_j \in \{-1,1\}$ such that $h(x_j^{\varepsilon_j}) > 1$ for all $j \leq k$. By the inductive hypothesis, there are elements $\varepsilon_{k+1},\dots,\varepsilon_n \in \{-1,1\}$ such that $1 \notin S(x_{k+1}^{\varepsilon_{k+1}},\dots,x_n^{\varepsilon_n})$. If $1 \in S(x_1^{\varepsilon_1},\dots,x_n^{\varepsilon_n})$, then $1 = h(1) > 1$, a contradiction. $\square$

An inmediate corollary:

Corollary 14.8. *Locally indicable groups are left-orderable.*

Another consequence of Burns–Hale's Theorem:

Exercise 14.9. Let G be a group and $\{N_\alpha : \alpha\}$ be a collection of normal subgroups of G such that $\cap_\alpha N_\alpha = \{1\}$. If G/N_α is left-ordererable for all α, then G is left-orderable.

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

A group G satisfies the **unique product property** if there are non-empty finite subsets A and B such that $|gA\cap B|=1$ for some $g\in G$. Thus G satisfies the unique product property if and only if for all finite non-empty subsets A and B there exists $g\in G$ such that $g=ab$ for unique elements $a\in A$ and $b\in B$.

Proposition 14.10. *A group with the unique product property is torsion-free.*

Proof. Assume that G has torsion and let $g\in G$ be an element of order $n\geq 2$. Let $A=B=\{1,g,g^2,\dots,g^{n-1}\}$. Then g admits more than one representation of the form $g=ab$ for $a\in A$ and $b\in B$, so G cannot have the unique product property. □

Proposition 14.11. *A left-orderable group satisfies the unique product property.*

Proof. Let G be a group and $A=\{a_1,\dots,a_n\}$ and $B=\{b_1,\dots,b_m\}$ be non-empty subsets of G. We may assume that $a_1<a_2<\cdots<a_n$ and $b_1<b_2<\cdots<b_m$. Let $g\in G$ be such that $ga_n=b_1$. Then $ga_1<ga_2<\cdots<ga_n=b_1<b_2<\cdots<b_m$. □

A group G satisfies the **double unique product property** if for any two given finite non-empty subsets A and B of G such that $|A|+|B|>2$ there exist at least two unique products in AB.

thm:Strojnowski

Theorem 14.12 (Strojnowski). *Sea G un grupo. Las siguientes afirmaciones son equivalentes:*

1) *G tiene la propiedad del doble producto único.*
2) *Para todo subconjunto $A\subseteq G$ finito y no vacío, existe al menos un producto único en $AA=\{a_1a_2 : a_1,a_2\in A\}$.*
3) *G tiene la propiedad del producto único.*

Proof. La implicación $(1)\implies(2)$ es trivial. Demostremos que vale $(2)\implies(3)$. Si G no tiene la propiedad del producto único, existen subconjuntos $A,B\subseteq G$ finitos y no vacíos tales que todo elemento de AB admite al menos dos representaciones. Sea $C=AB$. Todo $c\in C$ es de la forma $c=(a_1b_1)(a_2b_2)$ con $a_1,a_2\in A$ y $b_1,b_2\in B$. Como $a_2^{-1}b_1^{-1}\in AB$, existen $a_3\in A\setminus\{a_2\}$ y $b_3\in B\setminus\{b_1\}$ tales que $a_2^{-1}b_1^{-1}=a_3^{-1}b_3^{-1}$. Luego $b_1a_2=b_3a_3$ y entonces

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

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

Demostremos ahora que (3) $\implies$ (1). Si G tiene la propiedad del producto único pero no tiene la propiedad del doble producto único, existen subconjuntos $A,B \subseteq G$ finitos y no vacíos con $|A|+|B|>2$ tales que en AB existe un único elemento ab con una única representación en AB. Sean $C=a^{-1}A$ y $D=Bb^{-1}$. Entonces $1 \in C\cap D$ y el elemento neutro 1 admite una única representación en CD (pues si $1=cd$ con $c=a^{-1}a_1 \neq 1$ y $d=b_1b^{-1}\neq 1$, entonces $ab=a_1b_1$ con $a\neq a_1$ y $b\neq b_1$). Sean $E=D^{-1}C$ y $F=DC^{-1}$. Todo elemento de EF se escribe como $(d_1^{-1}c_1)(d_2c_2^{-1})$. Si $c_1\neq 1$ o $d_2\neq 1$ entonces $c_1d_2=c_3d_3$ para algún $c_3\in C\setminus\{c_1\}$ y algún $d_3\in D\setminus\{d_2\}$. Entonces $(d_1^{-1}c_1)(d_2c_2^{-1})=(d_1^{-1}c_3)(d_3c_2^{-1})$ son dos representaciones distintas para $(d_1^{-1}c_1)(d_2c_2^{-1})$. Si $c_2\neq 1$ o $d_1\neq 1$ entonces $c_2d_1=c_4d_4$ para algún $d_4\in D\setminus\{d_1\}$ y algún $c_4\in C\setminus\{c_2\}$ y entonces, como $d_1^{-1}c_2^{-1}=d_4^{-1}c_4^{-1}$, $(d_1^{-1}1)(1c_2^{-1})=(d_4^{-1}1)(1c_4^{-1})$. Como $|C|+|D|>2$, C o D contienen algún $c\neq 1$, y entonces $(1\cdot 1)(1\cdot 1)=(1\cdot c)(1\cdot c^{-1})$. Demostramos entonces que todo elemento de EF tiene al menos dos representaciones. □

Exercise 14.13. Demuestre que si G es un grupo que satisface la propiedad del producto único, entonces $K[G]$ tiene solamente unidades triviales.

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

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

Definition 14.14. Un grupo G se dice **difuso** si para todo subconjunto $A\subseteq G$ tal que $2\leq|A|<\infty$ se tiene $|\Delta(A)|\geq 2$.

Lemma 14.15. *Si G es ordenable a derecha, entonces G es difuso.*

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

lemma:difuso=>2up

Lemma 14.16. *Si G es difuso, entonces G tiene la propiedad del doble producto único.*

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

B

The braid group.

C

Kaplanski's problems.

D

The following result proves that the structure groups of finite solutions are left-orederable if and only if they are locally indicable.

Theorem 14.17 (Chiswell–Kropholler). *A left-orderable solvable group is locally indicable.*

See [23] for the proof.

Since structure groups of finite involutive solutions are solvable, the following corollary follows:

cor:LO<=>LI **Corollary 14.18.** *Let (X,r) be a finite involutive solution. Then $G(X,r)$ is left-ordered if and only if $G(X,r)$ is locally indicable.*

Our aim is to characterize involutive multipermutation solutions in terms of the left-orderability of the structure group. Let us start with an example.

exa:Navas **Example 14.19.** Let $X=\{1,2,3,4\}$ and $r\colon X\times X\to X\times X$, $r(x,y)=(\sigma_x(y),\tau_y(x))$, where

$$\begin{aligned} &\sigma_1=(12), && \sigma_2=(1324), && \sigma_3=(34), && \sigma_4=(1423),\\ &\tau_1=(14), && \tau_2=(1243), && \tau_3=(23), && \tau_4=(1342). \end{aligned}$$

The group

$$G(X,r)=\langle a,b,c,d : a^2=bd, ac=ca, ad=dc, ba=cb, b^2=d^2, c^2=db\rangle$$

is not left-orderable. Let $\deg\colon G(X,r)\to\mathbb{Z}$ be the degree of $G(X,r)$ and

$$K=\ker(\deg)=\langle a^{-1}b,a^{-1}c,a^{-1}d,b^{-1}c,b^{-1}d,c^{-1}d\rangle.$$

Write $p=a^{-1}b$, $q=a^{-1}c$, $r=a^{-1}d$, $s=b^{-1}c$, $t=b^{-1}d$ and $u=c^{-1}d$. Then

$$ps=q,\quad qu=r,\quad su=t,\quad pr=q^{-1},\quad qs=u,\quad st=p.$$

To prove that $G(x,r)$ is not left-orderable it is enough to prove that $G(X,r)$ is not locally indicable. Suppose on the contrary that there exists a group homomorphism $\phi\colon K \to \mathbb{R}$. Since

$$\det \begin{pmatrix} 1 & -1 & 0 & 1 & 0 & 0 \\ 0 & 1 & -1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & -1 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & -1 & -1 & 0 \end{pmatrix} = 16 \neq 0,$$

the linear system

$$\begin{aligned} 0 &= \phi(p) - \phi(q) + \phi(s), \\ 0 &= \phi(q) - \phi(r) + \phi(u), \\ 0 &= \phi(s) - \phi(t) + \phi(u), \\ 0 &= \phi(p) + \phi(q) + \phi(r), \\ 0 &= \phi(q) - \phi(s) - \phi(u), \\ 0 &= \phi(p) - \phi(s) - \phi(t), \end{aligned}$$

has only the trivial solution. Thus ϕ is the zero homomorphism and hence $G(X,r)$ is not left-orderable by Corollary 14.18.

thm:MP

Theorem 14.20. *Let (X,r) be a finite involutive solution. The following statements are equivalent:*

1) *(X,r) is multipermutation.*
2) *$G(X,r)$ is poly-$\mathbb{Z}$.*
3) *$G(X,r)$ is left-orderable*
4) *$G(X,r)$ is diffuse.*

Proof. Since (X,r) is not retractable, there exist $x,y \in X$ such that $x \neq y$ and $\sigma_x = \sigma_y$. Let $K = \langle x,y \rangle \cap \ker \deg$. The sequence

$$1 \longrightarrow K \longrightarrow G(X,r) \xrightarrow{\deg} \mathbb{Z} \longrightarrow 1$$

is exact. Since K is isomorphic to a subgroup of $\mathbb{Z}^X$, K is left-ordetable. Thus $G(X,r)$ is left-orderable by Proposition 13.18. □

Exercises

Open problems

Open problem 14.1 (?). Is there a non-diffuse group with the unique product property?

Notes

Example 14.19 goes back to Navas.

Theorem 14.20 is the joint work of different people. The implication $1) \implies 2)$ was first proved by Jespers and Okniński in [], see also [43]. Chouraqui independently proved that $1) \implies 3)$ in [25]. In [9] Bachiller, Cedó and Vendramin proved that $3) \implies 1)$. The equivalence between $1)$ and $4)$ was proved by Lebed and Vendramin in [47].

Chapter 15
Transitive groups

transitive

A

B

The classification of transitive groups of small degree can be used to produce quandles...

thm:quandles

Theorem 15.1.

Proof. □

C

Definition 15.2. A finite solution (X,r) is said to be **decomposable** if there is a decomposition $X = X_1 \cup X_2$ of X into a disjoint union of non-empty subsets X_1 and X_2 such that $r(X_1 \times X_1) \subseteq X_1 \times X_2$ and $r(X_2 \times X_2) \subseteq X_2 \times X_2$. A solution (X,r) is then **indecomposable** if it is not decomposable.

If (X,r) is a finite decomposable solution and $X = X_1 \cup X_2$ is a decomposition, then the restrictions $r|_{X_1 \times X_1}$ and $r|_{X_2 \times X_2}$ are solutions. Moreover, it follows that $r(X_1 \times X_2) \subseteq X_2 \times X_1$ and $r(X_2 \times X_1) \subseteq X_1 \times X_2$, see Exercise 15.1.

Proposition 15.3. *A finite solution (X,r) is indecomposable if and only if the group*

$$\langle \sigma_x, \tau_x : x, y \in X \rangle$$

acts transitively on X.

Proof. Let us assume that $X = X_1 \cup X_2$ is a decomposition of X into non-empty orbits... □

Note that this group is in general not isomorphic to the permutation group of the solution.

Definition 15.4. A finite solution (X,r) is said to be **simple** if $|X|>1$ and for every surjective homomorphism $f\colon (X,r)\to(Y,s)$ of solutions either f is an isomorphism or $|Y|=1$.

Example 15.5.

Example 15.6.

Example 15.7.

:simple=>indecomposable

Proposition 15.8. *Let (X,r) be a finite simple solution. If $|X|>2$, then (X,r) is indecomposable.* $\boxed{\textit{involutive?}}$

Proof. Let us assume that (X,r) is decomposable. Decompose $X=X_1\cup X_2$ for non-empty disjoint subsets X_1 and X_2 of X such that $r(X_i\times X_i)\subseteq X_i\times X_i$ for $i\in\{1,2\}$. Let $Y=\{1,2\}$ and $s\colon Y\times Y\to Y\times Y$, $s(x,y)=(y,x)$. Since $X=X_1\cup X_2$ is a decomposition, it follows that $r(X_i\times X_j)\subseteq X_j\times X_i$ for all $i,j\in\{1,2\}$. $\boxed{\text{Why?}}$ Let $f\colon X\to Y$, $f(x)=i$ if $x\in X_i$. Since f is then a surjective homomorphism of solutions and f is not an isomorphism (because $|X|>2$), the simplicity of (X,r) implies that $|Y|=1$, a contradiction. □

Proposition 15.9. *Let (X,r) be a finite simple* $\boxed{\textit{involutive}}$ *solution. If $|X|$ is not a prime number, then (X,r) is irretractable.*

Proof. Let us assume that (X,r) is retractable. Let $(X,r)\to\operatorname{Ret}(X,r)$, $x\mapsto[x]$, be the canonical map. Since it is a surjective homomorphism of solutions and (X,r) is retractable, the simplicity of (X,r) implies that $|\operatorname{Ret}(X,r)|=1$. Therefore (X,r) is a permutation solution, say $r(x,y)=(\sigma(y),\tau(x))$ for some commuting permutations $\sigma\colon X\to X$ and $\tau\colon X\to X$. Since $|X|>2$, the solution (X,r) is indecomposable by Proposition 15.8. This implies that σ is a cycle of length $|X|$ and $\tau=\sigma^k$ for some $k\in\mathbb{Z}$. Let us assume that $\sigma=(x_1\cdots x_n)$, where $n=|X|$. Since n is not a prime number, $n=dm$ for some $1<d<n$. Let $Y=\mathbb{Z}/(d)$ and $s\colon Y\times Y\to Y\times Y$, $s(i,j)=(j+1,i+k)$. Then (Y,s) is a solution. The map $f\colon X\to Y$, $f(x_i)=i \bmod d$ satisfies $f(\tau_{x_j}(x_i))=i+k$ and

$$f(\sigma_{x_i}(x_j))=\begin{cases} f(x_{j+1}) & \text{if } j<n,\\ 1 & \text{if } j=n.\end{cases}$$

Then a straightforward computation shows that f is a surjective homomorphism of solutions, a contradiction. □

The previous proposition cannot be extended to the non-involutive case.

Example 15.10. Let $X=\{1,\dots,6\}$. The permutation solution with permutations $\sigma=(153)(264)$ and $\tau=(12)(34)(56)$ is indecomposable.

D

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

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

This means that the operation is

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

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

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

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

Exercise 15.11. The group $\mathrm{Hol}(A)$ acts transitively on A and the stabilizer $a\in A$ is isomorphic to $\mathrm{Aut}(A)$.

A subgroup G of $\mathrm{Hol}(A)$ 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

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

lem:bijective **Lemma 15.12.** *If G is a regular subgroup of $\mathrm{Hol}(A)$, then $\pi_1\colon G\to A$ is bijective.*

Proof. 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 $\pi_2|_G(a,f^{-1})=a$. $\square$

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

thm:regular **Theorem 15.13.** *If A is a brace, then $\Delta = \{(a,\lambda_a) : a\in A\}$ is a regular subgroup of $\mathrm{Hol}(A,+)$. Conversely, if A is an additive group and G is a regular subgroup of $\mathrm{Hol}(A)$, 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 (4.2) 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 Lemma 15.12, 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 $a,b,c\in A$. $\square$

The following lemma is from [10].

lem:BNY

Lemma 15.14. *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 $(a,f)\in H$,

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

pro:regular

Proposition 15.15. *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 15.14 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 15.12. 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. $\square$

Now we present algorithm used to enumerate braces. It is based on Theorem 15.13. The use of Lemma 15.14 in Proposition 15.15 significantly improves the performance.

alg:regular

Algorithm 15.16. Let A be a finite group. To construct all braces with additive group A we proceed as follows:

1) Compute the holomorph $\mathrm{Hol}(A)$ of A.
2) Compute the list of regular subgroups of $\mathrm{Hol}(A)$ of order $|A|$ up to conjugation.
3) For each representative G of regular subgroups of $\mathrm{Hol}(A)$ construct the map $p\colon A \to G$ given by $a \mapsto (a, f) \in G$. Then the set A is a brace with additive group A and multiplication given by $a \circ b = p^{-1}(p(a)p(b))$ for all $a, b \in A$.

To enumerate all isomorphism classes of braces structures with a fixed additive group the third step of Algorithm 15.16 is not needed. Algorithm 15.16 can be used to compute the number $s(n)$ of non-isomorphic braces of size n. With small modifications it could be used to compute the number $a(n)$ of non-isomorphic braces of abelian type of size n, or the number of non-isomorphic radical rings, or the number of non-isomorphic braces of nilpotent type. Some values for $s(n)$ and $a(n)$ appear in Table 15.1.

Open problems

Open problem 15.1. Estimate $s(n)$ and $a(n)$ for $n \to \infty$.

Open problem 15.2. Construct and enumerate braces of size 64, 96, 128 and 160.

Notes

Theorem 15.13 was first observed by Catino and Rizzo [17] and Bachiller [7].

Table 15.1: 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

Algorithm 15.16 and most of the numbers of Table 15.1 appeared in [37]. It should be noted that the number of braces of size 57 of [37] is incorrect; the correct value is $s(57) = 8$, as Table 15.1 shows. Lemma 15.14 appears in [10] and it is needed to compute the number $a(n)$ of isomorphism classes of braces of abelian type of size $n \in \{32, 81, 96, 144, 160, 162\}$ and the number $s(n)$ of isomorphism classes of braces of size $n \in \{32, 54, 80, 81, 108, 112, 120, 136, 144, 147, 150, 152, 162, 168\}$.

Exercises

prob:decomposition

15.1. Let (X,r) be a finite decomposable solution and $X = X_1 \cup X_2$ be a decomposition. Prove that $r(X_1 \times X_2) \subseteq X_2 \times X_1$ and $r(X_2 \times X_1) \subseteq X_1 \times X_2$. Solution?

15.2. Let (X,r) be a finite involutive permutation solution. Prove that (X,r) is indecomposable if and only if σ is a cycle of length $|X|$.

Open problems

Open problem 15.3. Construct indecomposable (involutive) solutions of small size.

Notes

With some variations Theorem 15.1 appears in several places, see for example... Algorithms based on this theorem were used in ... and ... to construct and enumerate indecomposable quandles of small size.

Indecomposable quandles are...

Chapter 16
The transfer map

transfer

A

Let G be a group and H be a finite index subgroup. We will define a group homomorphism $G \to H/[H,H]$, known as the **transfer map** of G on H. Fix a **left transversal** T of H in G.

lem:sigma

Lemma 16.1. *Let G be a group and H be a subgroup of finite index $n = (G:H)$. Let $S = \{s_1, \dots, s_n\}$ and $T = \{t_1, \dots, t_n\}$ be transversals of H in G. If $g \in G$, there exist unique $h_1, \dots, h_n \in H$ and a permutation $\sigma \in \mathbb{S}_n$ such that*

$$gt_i = s_{\sigma(i)}h_i, \quad i \in \{1, \dots, n\}.$$

Proof. If $i \in \{1, \dots, n\}$, then there exists a unique $j \in \{1, \dots, n\}$ such that $gt_i \in s_jH$. Thus there exists a unique $h_i \in H$ such that $gt_i = s_jh_i$. Take $\sigma(i) = j$ and thus there is a well-defined map $\sigma \colon \{1, \dots, n\} \to \{1, \dots, n\}$. To prove that $\sigma \in \mathbb{S}_n$ it is enough to check that σ is injective. If $\sigma(i) = \sigma(k) = j$, since $gt_i = s_jh_i$ and $gt_k = s_jh_k$, it follows that $t_i^{-1}t_k = h_i^{-1}h_k \in H$. Hence $i = k$, as $t_iH = t_kH$. $\square$

Let G be a group and H be a subgroup of G of finite index n. If $T = \{t_1, \dots, t_n\}$ is a transversal of H in G, we define the map

$$\nu_T \colon G \to H/[H,H], \quad \nu_T(g) = \prod_{i=1}^{n} h_i$$

where $gt_i = t_jh_i$. Note that the product is well-defined since $H/[H,H]$ is an abelian group. We now prove that the map does not depend on the transversal.

lem:nu_T

Lemma 16.2. *Let G be a group and H be a subgroup of G of finite index. if T and S are transversal of H in G, then $\nu_T = \nu_S$.*

Proof. Assume that $gs_i = s_{\sigma(i)}h_i$ for all i. Write $s_i = t_ik_i$, $k_i \in H$. If $l_i = k_{\sigma(i)}h_ik_i^{-1}$, then

$$gt_i = gs_ik_i^{-1} = s_{\sigma(i)}h_ik_i^{-1} = t_{\sigma(i)}k_{\sigma(i)}h_ik_i^{-1} = t_{\sigma(i)}l_i$$

for all $i \in \{1,\dots,n\}$. Moreover,

$$s_{\sigma(i)}^{-1}gs_i = k_{\sigma(i)}^{-1}t_{\sigma(i)}^{-1}gt_ik_i.$$

Since $H/[H,H]$ is abelian,

$$\begin{aligned}\nu_S(g) &= \prod_{i=1}^n s_{\sigma(i)}^{-1}gs_i = \prod_{i=1}^n k_{\sigma(i)}^{-1}t_{\sigma(i)}^{-1}gt_ik_i\\ &= \prod_{i=1}^n k_{\sigma(i)}^{-1}\prod_{i=1}^n k_i\prod_{i=1}^n t_{\sigma(i)}^{-1}gt_i = \prod_{i=1}^n t_{\sigma(i)}^{-1}gt_i = \nu_T(g).\end{aligned}$$ □

By Lemma 16.2, if H is a finite-index subgroup of G, the map

$$\nu\colon G \to H/[H,H], \quad \nu(g) = \nu_T(g),$$

where T is some transversal of H in G, is well-defined.

theorem:transfer

Theorem 16.3. *Let G be a group and H be a finite-index subgroup of G. Then $\nu(xy) = \nu(v)\nu(y)$ for all $x,y \in G$.*

Proof. Let $T = \{t_1,\dots,t_n\}$ be a transversal of H in G. Let $x,y \in G$. By Lemma 16.1, there exist unique elements $h_1,\dots,h_n,k_1,\dots,k_n \in H$ and there are permutations $\sigma,\tau \in \mathbb{S}_n$ such that $xt_i = t_{\sigma(i)}h_i$ and $yt_i = t_{\tau(i)}k_i$. Since

$$xyt_i = xt_{\tau(i)}k_i = t_{\sigma\tau(i)}h_{\tau(i)}k_i$$

and $H/[H,H]$ is abelian,

$$\nu(xy) = \prod_{i=1}^n h_{\tau(i)}k_i = \prod_{i=1}^n h_{\tau(i)}\prod_{i=1}^n k_i = \nu(x)\nu(y).$$ □

If G is a group and H is a finite-index subgroup of G, the **transfer homomorphism** is the group homomorphism $\nu\colon G \to H/[H,H]$, $\nu(g) = \nu_T(g)$, for some transversal T of H in G.

lem:evaluation

Lemma 16.4. *Let G be a group and H be a subgroup of G with $(G:H) = n$. Let $T = \{t_1,\dots,t_n\}$ be a transversal of H in G. For each $g \in G$ there exists $m \in \mathbb{N}$, elements $s_1,\dots,s_m \in T$ and positive integers $n_1,\dots,n_m$ such that*

$$s_i^{-1}g^{n_i}s_i \in H, \quad n_1+\cdots+n_m = n \quad \textit{and} \quad \nu(g) = \prod_{i=1}^m s_i^{-1}g^{n_i}s_i.$$

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

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

of disjoint cycles.

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

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

it follows that

$$\begin{aligned} t_{j_1}^{-1} g^{n_i} g t_{j_1} &= t_{j_1}^{-1} g^{n_i - 1} g t_{j_1} \\ &= t_{j_1}^{-1} g^{n_i-1} t_{j_2} h_1 \\ &= t_{j_1}^{-1} g^{n_i-2} g t_{j_2} h_1 \\ &= t_{j_1}^{-1} g^{n_i-2} t_{j_3} h_2 h_1 \\ &\ \ \vdots \\ &= t_{j_1}^{-1} g t_{j_{n_i}} h_{n_{i-1}} \cdots h_2 h_1 \\ &= h_{j_1}^{-1} t_{j_1} h_{n_i} \cdots h_2 h_1 \in H. \end{aligned}$$

So we let $s_i = t_{j_1} \in T$. Now the claim follows, since $\nu(g) = h_1 \cdots h_n$. □

`prop:v(g)=g^n` **Proposition 16.5.** *Let G be a group and H be a central subgroup of index n. Then $\nu(g) = g^n$ for all $g \in G$.*

Proof. Let $g \in G$. By Lemma 16.4, there exist $s_1,\dots,s_m \in H$ such that $s_i^{-1} g^{n_i} s_i \in H$ and $\nu(g) = \prod_{i=1}^m s_i^{-1} g^{n_i} s_i$. Since H is central in G, then it is normal in G. Thus

$$g^{n_i} = s_i (s_i^{-1} g^{n_i} s_i) s_i^{-1} \in H \subseteq Z(G)$$

and hence

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

`xca:[x,y]^n=1` **Exercise 16.6.** Let G be a group such that $(G : Z(G)) = n$. If $x, y \in G$, then $[x,y]^n = 1$.

Another application.

`prop:semidirecto` **Proposition 16.7.** *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, $H = H/[H,H]$ and the transfer map is $\nu \colon G \to H$. By Lemma 16.4,

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

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 $H \hookrightarrow G \xrightarrow{\nu} H$ is a group homomorphism. We claim that it is an isomorphism. It is injective: If $h^n = 1$, then $|h|$ divides $|H|$ and divides 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 $\nu(h^m) = h^{nm} = h$.

Therefore $G \simeq N \rtimes H$, as N is normal in G, $N \cap H = \{1\}$ and $G = NH$ (because $|NH| = |N||H|$ and $G/N \simeq H$). □

Exercise 16.8. 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.

Theorem 16.9. *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 $\varepsilon \colon G \to \mathrm{Aut}(K)$. Since $\mathrm{Aut}(K) \simeq \mathrm{Aut}(\mathbb{Z}) = \{-1, 1\}$, there are two cases to consider.

Assume first that $\varepsilon = \mathrm{id}$. Since $K \subseteq Z(G)$, let $\nu \colon G \to K$ be the transfer homomorphism. By Proposition 16.5, $\nu(g) = g^n$, 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 $\varepsilon \neq \mathrm{id}$. Let $N = \ker \varepsilon \neq G$. Since $K \simeq \mathbb{Z}$ is abelian, $K \subseteq N$. The result proved in the previous paragraph applied to $\varepsilon|_N = 1$ 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. □

B

As an application of the transfer map we will prove several theorems about the commutator subgroup. We start with the following result which of course it is of independ interest.

theorem:Dietzmann

Theorem 16.10 (Dietzmann). *Let G be a group and $X \subseteq G$ be a finite subset of G closed under conjugation. If there exists $n \in \mathbb{N}$ such that $x^n = 1$ for all $x \in X$, then $\langle X \rangle$ is a finite subgroup of G.*

Proof. Let $S = \langle X \rangle$ be the subgroup generated by X. 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 representation of s, then s is a product of m elements of X where the first k elements are equal to x. Assume that

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

where each $x_j \neq x$ 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 our x. The same argument implies that s can be written as

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

where the y_j are elements of $X \setminus \{x\}$.

Let $s \in S$. Write s as a product of m elements of X, where m is minimal. To see that S is finite it is enough to show that $m \leq (n-1)|X|$.

If $m > (n-1)|X|$, then at least one $x \in X$ appears n times in the representation of s. Without loss of generality, write

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

a contradiction to the minimality of m. □

To prove Schur's theorem on the commutator subgroup we need a lemma.

lemma:[s,t]

Lemma 16.11. *Let G be a group and T be a transversal of $Z(G)$ in G. Then each commutator of G is of the form $[s,t]$ for $s,t \in T$. In particular, G has a finite number of commutators if $Z(G)$ is of finite index.*

Proof. Every element of G is of the form sx for $s \in T$ and $x \in Z(G)$. To prove the first claim note that $[sx,ty] = [s,t]$, as $x,y \in Z(G)$. The second claim now follows from $|T| = (G : Z(G))$. □

We now prove Schur's theorem.

theorem:Schur_commutador

Theorem 16.12 (Schur). *If $Z(G)$ has finite index in G, then $[G,G]$ is finite.*

Proof. Let $X = \{[x,y] : x,y \in G\}$. By Lemma 16.11), X is finite. Moreover, X is closed under conjugation,

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

for all $g,x,y \in G$. If $n = (G : Z(G))$, then $x^n = 1$ for all $x \in X$ by Exercise 16.6. Thus the claim follows from Dietzmann's theorem. □

Some applications.

thm:Niroomand

Theorem 16.13 (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

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

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 16.14 (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 $G/Z(G) = \langle x_1Z(G),\dots,x_nZ(G)\rangle$. 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 $g = x_kz$ for some $k \in \{1,\dots,n\}$ and some $z \in Z(G)$, it follows that

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

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

Exercise 16.15. Prove Theorem 16.14 from Theorem 16.13.

C

lem:normal_complement

Lemma 16.16. *Let G be a finite group and p be a prime number dividing the order of G. Let $P \in \mathrm{Syl}_p(G)$. If $g,h \in C_G(P)$ are conjugate in G, then they are conjugate in $N_G(P)$.*

Proof. Let $x \in G$ be such that $g = xhx^{-1}$. Then $g \in C_G(xPx^{-1})$ and hence P and xPx^{-1} are Sylow subgroups of $C_G(g)$. By the second Sylow's theorem, there exists $c \in C_G(g)$ such that $P = cxP(cx)^{-1}$. Theredfore $cx \in N_G(P)$ and

$$(cx)h(cx)^{-1} = c(xhx^{-1})c^{-1} = cgc^{-1} = g. \qquad \square$$

Let G be a finite group and p a prime number dividing the order of G. A **normal p-complement** is a normal subgroup N of G of order not divisible by p and such that $(G:N)$ is a power of p. We say that G is **p-nilpotent** if G contains a normal p-complement.

Proposition 16.17. *If the group G admits a normal p-complement N, then N is a characteristic subgroup of G.*

Proof. Assume that $|G| = p^\alpha n$, where $\gcd(n,p) = 1$. Let $\pi\colon G \to G/N$ be the canonical map. Then $|N| = n$. We claim that N is the unique subgroup of G of order n. If K is a subgroup of G of order n, then $\pi(K) \simeq K/K \cap N$ and hence $|\pi(K)|$ divides n. Since $\pi(K)$ is a subgroup of G/N, it follows that $|\pi(K)|$ divides p. Thus $\pi(K)$ is trivial and hence $K = N$ and G contains a unique subgroup of order n. In particular, N is characteristic in G. $\square$

rnside:normal_complement

Theorem 16.18 (Burnside). *Let G be a finite group and p be a prime number dividing the order of G. Let $P \in \mathrm{Syl}_p(G)$ be such that $P \subseteq Z(N_G(P))$. Then G is p-nilpotent.*

Proof. Since P is abelian, let $\nu\colon G \to P$ be the transfer map. Let $g \in P$. By Lemma 16.4, there exist $s_1,\dots,s_m \in G$ and $n_1,\dots,n_m$ such that $n_1 + \cdots + n_m = n$, $s_i^{-1} g^{n_i} s_i \in P$ and

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

Since P is abelian, $P \subseteq C_G(P)$. By Lemma 16.16, there exist elements $c_i \in N_G(P)$ such that

$$s_i^{-1} g^{n_i} s_i = c_i^{-1} g^{n_i} c_i.$$

Thus $s_i^{-1}g^{n_i}s_i = g_i^{n_i}$, as $P \subseteq Z(N_G(P))$. Therefore $\nu(g) = g^n$, where $n = (G:P)$. Since n and $|P|$ are coprime, there exist $r,s \in \mathbb{Z}$ such that $rn + s|P| = 1$. Thus the restriction $\nu|_P$ is surjective, as

$$g = (g^r)^n = \nu(g^r).$$

By the isomorphism theorem, $P/\ker\nu \cap P \simeq \nu(P) = P$. Thus $\ker\nu \cap P = \{1\}$. Moreover, $\nu(G) = \nu(P)$, as $P \supseteq \nu(G) \supseteq \nu(P) = P$.

We now claim that $\ker\nu$ is a normal p-complement in G. Indeed, $\ker\nu$ is normal in G. Since $(G:\ker\nu) = |\nu(G)| = |P|$ and P is a Sylow p-subgroup, $\ker\nu$ has order coprime with p. □

We now prove an interesting corollary. We shall need the following lemma.

lem:NC **Lemma 16.19.** *Sea G un grupo y H un subgrupo de G. Entonces $C_G(H)$ es un subgrupo normal de $N_G(H)$ y $N_G(H)/C_G(H)$ es isomorfo a un subgrupo de* $\mathrm{Aut}(H)$.

Proof. Sea $\phi\colon N_G(H) \to \mathrm{Aut}(H)$, $\phi(g) = c_g|H$, donde $c_g(h) = ghg^{-1}$. La función ϕ está bien definida (pues su dominio es $N_G(H)$) y es morfismo de grupos. Como $\ker\phi = C_G(H)$, se tiene que $C_G(H)$ es normal en $N_G(H)$. Por el primer teorema de isomorfismo, $N_G(H)/C_G(H) \simeq \phi(N_G(H)) \leq \mathrm{Aut}(H)$. □

Now we prove the following corollary of Burnside's theorem.

cor:Sylow_ciclico **Corollary 16.20.** *Let G be a finite group and p be the smallest prime divisor of $|G|$. If some $P \in \mathrm{Syl}_p(G)$ is cyclic, then G is p-nilpotent.*

Proof. Assume that $|P| = p^m$. By Lemma 16.19, $N_G(P)/C_G(P)$ is isomorphic to a subgroup of $\mathrm{Aut}(P)$. Since P is cyclic, $|N_G(P)/C_G(P)|$ divides

$$|\mathrm{Aut}(P)| = \phi(|P|) = p^{m-1}(p-1).$$

Since $P \subseteq C_G(P)$, p is coprime with $|N_G(P)/C_G(P)|$. Thus $|N_G(P)/C_G(P)|$ divides $p-1$. Since p is the smallest prime divisor of $|G|$, it follows that $p-1$ and $|G|$ are coprime. Moreover, $|N_G(P)/C_G(P)|$ divides $|G|$ and hence $|N_G(P)/C_G(P)| = 1$. Therefore $N_G(P) = C_G(P)$.

Since P is abelian, $P \subseteq Z(C_G(P)) = Z(N_G(P))$. Burnside's theorem implies that G is p-nilpotent. □

A **Z-group** is a group such that all its Sylow subgroups are cyclic.

Exercise 16.21. Prove that Z-groups are solvable.

The previous exercise show in particular that finite groups of square-free order are always solvable.

Theorem 16.22. *Let G be a finite non-abelian simple group and p be the smallest prime divisor of $|G|$. Then either p^3 divides $|G|$ or 12 divides $|G|$.*

Proof. Sea $P \in \mathrm{Syl}_p(G)$. By Corollary 16.20, P is not cyclic and then $|P| \geq p^2$. If p^3 does not divide $|G|$, $P \simeq C_p \times C_p$ is a two-dimensional vector space over the field $\mathbb{F}_p$. Since $|N_G(P)/C_G(P)|$ divides $|G|$, all prime divisors of $|N_G(P)/C_G(P)|$ are $\geq p$. Since $N_G(P)/C_G(P)$ is isomorphic to a subgroup of $\mathrm{Aut}(P)$ by Lemma 16.19 and $\mathrm{Aut}(P) \simeq \mathbf{GL}_2(p)$ has order

$$(p^2-1)(p^2-p) = p(p+1)(p-1)^2,$$

it follows that $|N_G(P)/C_G(P)|$ divides $p(p+1)(p-1)^2$.

Since P is abelian, $P \subseteq C_G(P)$. Thus $|N_G(P)/C_G(P)|$ is coprime with p and hence $|N_G(P)/C_G(P)|$ divides $(p+1)(p-1)^2$. Since p is the smallest prime divisor of $|G|$, the numbers $p-1$ and $|N_G(P)/C_G(P)|$ are coprime. Thus $|N_G(P)/C_G(P)|$ divides $p+1$. Burnside's theorem implies that $|N_G(P)/C_G(P)| \neq 1$. Hence $p=2$ because if p is odd, the smallest prime divisor of $|N_G(P)/C_G(P)|$ is $\geq p+2$. We conclude that $|N_G(P)/C_G(P)| = 3$ and hence $|G|$ is divisible by $12 = 2^2 3$. □

theorem:[GG]PZNG(P)=1

Theorem 16.23. *Let G be a finite group and P be an abelian Sylow subgroup of G. Then $[G,G] \cap P \cap Z(N_G(P)) = \{1\}$.*

Proof. Sea $x \in [G,G] \cap P \cap Z(N_G(P))$ y sea $\nu \colon G \to P$ el morfismo de transferencia. Por el lema **??** existen $s_1, \dots, s_m \in G$ y existen $n_1, \dots, n_m$ tales que $n_1 + \cdots + n_m = (G:P)$, $s_i^{-1} g^{n_i} s_i \in P$ y

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

Como P es abeliano, $P \subseteq C_G(P)$. Entonces x^{n_i} y $s_i^{-1} x^{n_i} s_i$ son conjugados en $N_G(P)$ por el lema **??**. Como x^{n_i} es central en $N_G(P)$ y $[G,G] \subseteq \ker \nu$, se concluye que $x = 1$ pues $1 = \nu(x) = x^{(G:P)}$ y $x \in P$. □

Corollary 16.24. *Sea G un grupo finito no abeliano y sea $P \in \mathrm{Syl}_2(G)$ tal que $P \simeq C_{a_1} \times \cdots \times C_{a_k}$ con $a_1 > a_2 \geq a_3 \geq \cdots \geq a_k \geq 2$. Entonces G no es simple.*

Proof. Sea $S = \{x^{n/2} : x \in P\}$. Es fácil ver que S es un subgrupo de P y que S es característico en P, es decir: $f(S) \subseteq S$ para todo $f \in \mathrm{Aut}(P)$. Como $S \simeq C_2$, podemos escribir $S = \{1, s\}$. Entonces $s \in Z(N_G(P))$ pues $gsg^{-1} \in S$ para todo $g \in N_G(P)$. Por el teorema 16.23, $s \notin [G,G]$ y luego $[G,G] \neq G$. Si G fuera simple, G sería abeliano pues $[G,G] = 1$. □

Vimos en el corolario **??** que todo grupo tal que todos sus subgrupos de Sylow son cíclicos es resoluble.

Un grupo G se dice *meta-cíclico* si G tiene un subgrupo normal N cíclico tal que G/N es cíclico.

Lemma 16.25. *Si G es un grupo resoluble, entonces $C_G(F(G)) = F(G)$.*

Proof. □

theorem:Z=>metacyclic

Theorem 16.26. *Todo Z-grupo es meta-cíclico.*

Proof. Sea G un Z-grupo. Por el corolario **??**, G es resoluble y entonces, por el lema, el subgrupo de Fitting $F(G)$ satisface $C_G(F(G)) \subseteq F(G)$.

Demostremos que $F(G)$ es cíclico. En efecto, como $F(G)$ es nilpotente, $F(G)$ es producto directo de sus subgrupos de Sylow. Como todo subgrupo de Sylow de $F(G)$ es un p-subgrupo de G, todo Sylow de $F(G)$ es cíclico (por estar contenido en algún subgrupo de Sylow de G).

Como $F(G)$ es cíclico, $F(G)$ es en particular abeliano y luego $F(G) \subseteq C_G(F(G))$. Si G actúa en $F(G)$ por conjugación, se tiene un morfismo $\gamma \colon G \to \operatorname{Aut}(F(G))$ tal que $\ker\gamma = C_G(F(G)) = F(G)$ (pues $\gamma_g(x) = gxg^{-1}$). En particular, $G/F(G)$ es abeliano por ser isomorfo a un subgrupo del grup abeliano $\operatorname{Aut}(F(G))$. Como además los subgrupos de Sylow de $G/F(G)$ son cíclicos (pues son cocientes de los subgrupos de Sylow de G), $G/F(G)$ es cíclico. □

D

Exercises

Open problems

Notes

References

1. E. Acri, R. Lutowski, and L. Vendramin. Retractability of solutions to the Yang-Baxter equation and p-nilpotency of skew braces. *Internat. J. Algebra Comput.*, 30(1):91–115, 2020.
2. O. Akgün, M. Mereb, and L. Vendramin. Enumeration of set-theoretic solutions to the Yang-Baxter equation, 2020.
3. B. Amberg, S. Franciosi, and F. de Giovanni. *Products of groups*. Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, 1992. Oxford Science Publications.
4. S. A. Amitsur. Nil radicals. Historical notes and some new results. In *Rings, modules and radicals (Proc. Internat. Colloq., Keszthely, 1971)*, pages 47–65. Colloq. Math. Soc. János Bolyai, Vol. 6, 1973.
5. N. Andruskiewitsch and M. Graña. From racks to pointed Hopf algebras. *Adv. Math.*, 178(2):177–243, 2003.
6. M. Ashford and O. Riordan. Counting racks of order n. *Electron. J. Combin.*, 24(2):Paper No. 2.32, 20, 2017.
7. D. Bachiller. Counterexample to a conjecture about braces. *J. Algebra*, 453:160–176, 2016.
8. D. Bachiller. Solutions of the Yang-Baxter equation associated to skew left braces, with applications to racks. *J. Knot Theory Ramifications*, 27(8):1850055, 36, 2018.
9. D. Bachiller, F. Cedó, and L. Vendramin. A characterization of finite multipermutation solutions of the Yang-Baxter equation. *Publ. Mat.*, 62(2):641–649, 2018.
10. V. G. Bardakov, M. V. Neshchadim, and M. K. Yadav. Computing skew left braces of small orders. *Internat. J. Algebra Comput.*, 30(4):839–851, 2020.
11. S. R. Blackburn. Enumerating finite racks, quandles and kei. *Electron. J. Combin.*, 20(3):Paper 43, 9, 2013.
12. M. Brešar. *Introduction to noncommutative algebra*. Universitext. Springer, Cham, 2014.
13. E. Brieskorn. Automorphic sets and braids and singularities. In *Braids (Santa Cruz, CA, 1986)*, volume 78 of *Contemp. Math.*, pages 45–115. Amer. Math. Soc., Providence, RI, 1988.
14. N. P. Byott. Nilpotent and abelian Hopf-Galois structures on field extensions. *J. Algebra*, 381:131–139, 2013.
15. N. P. Byott. Solubility criteria for Hopf-Galois structures. *New York J. Math.*, 21:883–903, 2015.
16. F. Catino, I. Colazzo, and P. Stefanelli. Skew left braces with non-trivial annihilator. *J. Algebra Appl.*, 18(2):1950033, 23, 2019.
17. F. Catino and R. Rizzo. Regular subgroups of the affine group and radical circle algebras. *Bull. Aust. Math. Soc.*, 79(1):103–107, 2009.
18. F. Cedó. Left braces: solutions of the Yang-Baxter equation. *Adv. Group Theory Appl.*, 5:33–90, 2018.
19. F. Cedó, T. Gateva-Ivanova, and A. Smoktunowicz. Braces and symmetric groups with special conditions. *J. Pure Appl. Algebra*, 222(12):3877–3890, 2018.

20. F. Cedó, E. Jespers, and J. Okniński. Retractability of set theoretic solutions of the Yang-Baxter equation. *Adv. Math.*, 224(6):2472–2484, 2010.
21. F. Cedó, E. Jespers, and J. Okniński. Braces and the Yang-Baxter equation. *Comm. Math. Phys.*, 327(1):101–116, 2014.
22. F. Cedó, A. Smoktunowicz, and L. Vendramin. Skew left braces of nilpotent type. *Proc. Lond. Math. Soc. (3)*, 118(6):1367–1392, 2019.
23. I. M. Chiswell and P. H. Kropholler. Soluble right orderable groups are locally indicable. *Canad. Math. Bull.*, 36(1):22–29, 1993.
24. F. Chouraqui. Garside groups and Yang-Baxter equation. *Comm. Algebra*, 38(12):4441–4460, 2010.
25. F. Chouraqui. Left orders in Garside groups. *Internat. J. Algebra Comput.*, 26(7):1349–1359, 2016.
26. A. Clay and D. Rolfsen. *Ordered groups and topology*, volume 176 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2016.
27. M. Deakonesku and G. L. Uolls. On the orbits of automorphism groups. *Sibirsk. Mat. Zh.*, 46(3):533–537, 2005.
28. P. Dehornoy. Set-theoretic solutions of the Yang-Baxter equation, RC-calculus, and Garside germs. *Adv. Math.*, 282:93–127, 2015.
29. V. G. Drinfel′d. On some unsolved problems in quantum group theory. In *Quantum groups (Leningrad, 1990)*, volume 1510 of *Lecture Notes in Math.*, pages 1–8. Springer, Berlin, 1992.
30. M. Elhamdadi and S. Nelson. *Quandles—an introduction to the algebra of knots*, volume 74 of *Student Mathematical Library*. American Mathematical Society, Providence, RI, 2015.
31. P. Etingof and S. Gelaki. A method of construction of finite-dimensional triangular semisimple Hopf algebras. *Math. Res. Lett.*, 5(4):551–561, 1998.
32. P. Etingof, T. Schedler, and A. Soloviev. Set-theoretical solutions to the quantum Yang-Baxter equation. *Duke Math. J.*, 100(2):169–209, 1999.
33. The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.11.1*, 2021.
34. T. Gateva-Ivanova. A combinatorial approach to the set-theoretic solutions of the Yang-Baxter equation. *J. Math. Phys.*, 45(10):3828–3858, 2004.
35. T. Gateva-Ivanova. Set-theoretic solutions of the Yang-Baxter equation, braces and symmetric groups. *Adv. Math.*, 338:649–701, 2018.
36. T. Gateva-Ivanova and M. Van den Bergh. Semigroups of *I*-type. *J. Algebra*, 206(1):97–112, 1998.
37. L. Guarnieri and L. Vendramin. Skew braces and the Yang-Baxter equation. *Math. Comp.*, 86(307):2519–2534, 2017.
38. J. Hoste and P. D. Shanahan. An enumeration process for racks. *Math. Comp.*, 88(317):1427–1448, 2019.
39. I. M. Isaacs. *Finite group theory*, volume 92 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, 2008.
40. I. M. Isaacs. Group actions and orbits. *Arch. Math. (Basel)*, 98(5):399–401, 2012.
41. N. Jacobson. The radical and semi-simplicity for arbitrary rings. *Amer. J. Math.*, 67:300–320, 1945.
42. E. Jespers, L. . Kubat, A. Van Antwerpen, and L. Vendramin. Factorizations of skew braces. *Math. Ann.*, 375(3-4):1649–1663, 2019.
43. E. Jespers and J. Okniński. *Noetherian semigroup algebras*, volume 7 of *Algebra and Applications*. Springer, Dordrecht, 2007.
44. G. Köthe. Die Struktur der Ringe, deren Restklassenring nach dem Radikal vollständig reduzibel ist. *Math. Z.*, 32(1):161–186, 1930.
45. J. Krempa. Logical connections between some open problems concerning nil rings. *Fund. Math.*, 76(2):121–130, 1972.
46. I. Lau. An associative left brace is a ring. *J. Algebra Appl.*, 19(9):2050179, 6, 2020.
47. V. Lebed and L. Vendramin. On structure groups of set-theoretic solutions to the Yang-Baxter equation. *Proc. Edinb. Math. Soc. (2)*, 62(3):683–717, 2019.
48. J.-H. Lu, M. Yan, and Y.-C. Zhu. On the set-theoretical Yang-Baxter equation. *Duke Math. J.*, 104(1):1–18, 2000.

49. H. Meng, A. Ballester-Bolinches, and R. Esteban-Romero. Left braces and the quantum Yang-Baxter equation. *Proc. Edinb. Math. Soc. (2)*, 62(2):595–608, 2019.
50. P. P. Nielsen. Simplifying Smoktunowicz's extraordinary example. *Comm. Algebra*, 41(11):4339–4350, 2013.
51. J. Pakianathan and K. Shankar. Nilpotent numbers. *Amer. Math. Monthly*, 107(7):631–634, 2000.
52. R. Plemmons. Construction and analysis of non-equivalent finite semigroups. In *Computational Problems in Abstract Algebra (Proc. Conf., Oxford, 1967)*, pages 223–228. Pergamon, Oxford, 1970.
53. S. D. Promislow. A simple example of a torsion-free, nonunique product group. *Bull. London Math. Soc.*, 20(4):302–304, 1988.
54. J. H. Przytycki. Distributivity versus associativity in the homology theory of algebraic structures. *Demonstratio Math.*, 44(4):823–869, 2011.
55. W. Rump. A decomposition theorem for square-free unitary solutions of the quantum Yang-Baxter equation. *Adv. Math.*, 193(1):40–55, 2005.
56. W. Rump. Braces, radical rings, and the quantum Yang-Baxter equation. *J. Algebra*, 307(1):153–170, 2007.
57. W. Rump. The brace of a classical group. *Note Mat.*, 34(1):115–144, 2014.
58. A. Smoktunowicz. Polynomial rings over nil rings need not be nil. *J. Algebra*, 233(2):427–436, 2000.
59. A. Smoktunowicz. On some results related to Köthe's conjecture. *Serdica Math. J.*, 27(2):159–170, 2001.
60. A. Smoktunowicz. Some results in noncommutative ring theory. In *International Congress of Mathematicians. Vol. II*, pages 259–269. Eur. Math. Soc., Zürich, 2006.
61. A. Smoktunowicz. A note on set-theoretic solutions of the Yang-Baxter equation. *J. Algebra*, 500:3–18, 2018.
62. A. Smoktunowicz. On Engel groups, nilpotent groups, rings, braces and the Yang-Baxter equation. *Trans. Amer. Math. Soc.*, 370(9):6535–6564, 2018.
63. A. Smoktunowicz and L. Vendramin. On skew braces (with an appendix by N. Byott and L. Vendramin). *J. Comb. Algebra*, 2(1):47–86, 2018.
64. A. Soloviev. Non-unitary set-theoretical solutions to the quantum Yang-Baxter equation. *Math. Res. Lett.*, 7(5-6):577–596, 2000.
65. Y. P. Sysak. Products of almost abelian groups. In *Investigations of groups with restrictions for subgroups (Russian)*, pages 81–85, iii. Akad. Nauk Ukrain. SSR, Inst. Mat., Kiev, 1988.
66. C. Tsang and C. Qin. On the solvability of regular subgroups in the holomorph of a finite solvable group. *Internat. J. Algebra Comput.*, 30(2):253–265, 2020.
67. P. Vojtěchovský and S. Y. Yang. Enumeration of racks and quandles up to isomorphism. *Math. Comp.*, 88(319):2523–2540, 2019.
68. M. Wada. Group invariants of links. *Topology*, 31(2):399–406, 1992.
69. A. Weinstein and P. Xu. Classical solutions of the quantum Yang-Baxter equation. *Comm. Math. Phys.*, 148(2):309–343, 1992.
70. E. Zelmanov. *Nil rings and periodic groups*. KMS Lecture Notes in Mathematics. Korean Mathematical Society, Seoul, 1992. With a preface by Jongsik Kim.

Index