Journal of Number Theory 190 (2018) 394–413

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

The L-algebra of Hurwitz primes

Wolfgang Rump

Institute for Algebra and Number Theory, University of Stuttgart, Pfaffenwaldring 57, D-70550 Stuttgart, Germany

ARTICLE INFO

Article history:
Received 13 September 2017
Received in revised form 7 March 2018
Accepted 8 March 2018
Available online 22 April 2018
Communicated by S.J. Miller

Dedicated to B. V. M.

MSC:
primary 11R52, 11R27, 81P10, 16U30, 20F60

Keywords:
Hurwitz prime
Metacommutation
L-algebra
Right ℓ-group
Garside group

ABSTRACT

Conway and Smith proved that up to recombination of conjugate primes and migration of units, the only obstruction to unique factorization in the ring of Hurwitz integers in the quaternions is *metacommutation* of primes with distinct norm. We show that the Hurwitz primes form a discrete L^*-algebra, a quantum structure which provides a general explanation for metacommutation. L-algebras arise in the theory of Artin–Tits groups, quantum logic, and in connection with solutions of the quantum Yang–Baxter equation. It is proved that every discrete L^*-algebra admits a natural embedding into a right ℓ-group, which yields a new class of Garside groups.

0. Introduction

Let $\mathbb{H} = \mathbb{R} \oplus \mathbb{R}i \oplus \mathbb{R}j \oplus \mathbb{R}k$ be the skew-field of quaternions. The reduced norm $N(\alpha) = \overline{\alpha}\alpha = t^2 + x^2 + y^2 + z^2$ of an element $\alpha = t + xi + yj + zk \in \mathbb{H}$ gives a group homomorphism $N \colon \mathbb{H}^\times \twoheadrightarrow \mathbb{R}^\times$, where $\overline{\alpha} := t - xi - yj - zk$ denotes the conjugate quaternion. The subring $H := \mathbb{Z}\varrho \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}k$ of *Hurwitz quaternions*, where $\varrho := \frac{1}{2}(1 + i + j + k)$,

E-mail address: rump@mathematik.uni-stuttgart.de.

https://doi.org/10.1016/j.jnt.2018.03.004
0022-314X/© 2018 Elsevier Inc. All rights reserved.

was introduced in the 19th century by Hurwitz [19], who proved that H is a left and right principal ideal domain. Its unit group $H^\times$ consists of the $\varepsilon \in H$ with $N(\varepsilon) = 1$, and $\pi \in H$ is a prime if and only if $N(\pi)$ is a rational prime. Up to multiplication by units in H, every odd rational prime p divides exactly $p+1$ Hurwitz primes which constitute a projective line $\mathbb{P}^1(\mathbb{F}_p)$. As H is non-commutative, unique factorization into primes cannot be expected, but Conway and Smith [8] proved that up to migration of units, the only obstructions are *recombination* $\overline{\pi}\pi = \overline{\sigma}\sigma$ of primes $\pi, \sigma \in H$ with the same norm, and another phenomenon which they called *metacommutation*. This means that up to migration of units, any product $\pi\sigma$ of Hurwitz primes with distinct odd norms can be uniquely rewritten as

$$\pi\sigma = \sigma'\pi'$$

such that $N(\pi') = N(\pi)$ and $N(\sigma') = N(\sigma)$. Metacommutation was analysed recently by Cohn and Kumar [8] who proved that the sign of the permutation $\pi \mapsto \pi'$ is independent of σ and equal to the Legendre symbol $\left(\frac{q}{p}\right)$, where $p := N(\pi)$ and $q := N(\sigma)$. Forsyth et al. [16] simplified the proof of this remarkable property.

In this paper, we explain metacommutation as a quantum phenomenon and exhibit a close relationship to a class of Garside groups [13,11,12]. More precisely, we show that metacommutation takes place in any L^**-algebra*, that is, an L-algebra [29] with a special involution. Conversely, we show that up to multiplication with units, the Hurwitz primes form an L^*-algebra. Before we can make this precise and discuss the special rôle of the ramified prime at 2, we give a brief sketch of some pertinent properties of L^*-algebras.

Recall that an L*-algebra* is a set X with a binary operation $\rightarrow$ and an element 1 such that $x \rightarrow x = x \rightarrow 1 = 1$ and $1 \rightarrow x = x$, and

$$(x \rightarrow y) \rightarrow (x \rightarrow z) = (y \rightarrow x) \rightarrow (y \rightarrow z)$$

holds for $x, y \in X$. Moreover, it is assumed that $x \rightarrow y = 1 = y \rightarrow x$ implies that $x = y$. The prototypical example of an L-algebra is the negative cone of a *right* ℓ*-group* [32], a group G with a lattice order such that the right multiplications are lattice automorphisms. The negative cone $G^- := \{a \in G \,|\, a \leqslant 1\}$ is an L-algebra with $a \rightarrow b := ba^{-1} \wedge 1$, and G with its lattice order can be recovered from the L-algebra G^-.

Important examples of right ℓ-groups are Artin–Tits groups [5,14], and other Garside groups [12] like the structure groups of non-degenerate unitary set-theoretic solutions of the quantum Yang–Baxter equation [15,22,6], right-ordered groups [9,35,4,25,26], structure groups of orthomodular lattices [34], and the various lattice-ordered groups arising in functional analysis [23,24] and elsewhere [1,10]. The *quasi-centre* of a right ℓ-group G, a concept which extends the same-named notion for Artin–Tits groups [5,14], consists of the elements $a \in G$ which are *normal* in the sense that $aG^-a^{-1} = G^-$. By [33], Proposition 5, the quasi-centre is a (two-sided) ℓ-group.

Not every L-algebra comes from a group, but it can be shown that any L-algebra X admits a universal map $q\colon X \rightarrow G(X)$ into a group, the *structure group* of X. Moreover, any L-algebra X has a partial order $x \leqslant y \ :\Longleftrightarrow\ x \to y = 1$, and 1 is always the greatest element of X. If the elements $x \neq 1$ are pairwise incomparable, the L-algebra X is said to be *discrete* [32]. The map $X \mapsto G(X)$ gives a one-to-one correspondence between finite discrete L-algebras X satisfying the stronger condition $x \to y = y \to x \Rightarrow x = y$ and modular Garside groups ([32], Theorem 5). The arrow notation is due to a logical interpretation of $\to$ as implication. Then $\leqslant$ stands for the entailment relation.

The structure group of an L-algebra X is obtained in two steps (see [29] for details). Firstly, X embeds into a *self-similar* L-algebra $S(X)$, equipped with a natural monoid structure (see Section 1). Secondly, $S(X)$ has a group of left fractions, namely, $G(X)$.

Now if X is a discrete L^*-algebra, the map $q\colon X \to G(X)$, which usually need not even be monotone, is an embedding so that $S(X)$ maps isomorphically onto the negative cone of $G(X)$, and the underlying lattice of $G(X)$ is modular (Theorem 1). The negative cone $S(X)$ is again an L^*-algebra, with a grading $S(X) = \bigsqcup_{n\in\mathbb{N}} S^n(X)$ such that $S^0(X) = \{1\}$ and $S^1(X) = X \smallsetminus \{1\}$. Moreover, Theorem 1 gives a quantum-theoretic explanation for the two phenomena encountered in the arithmetic of Hurwitz primes. In this analogy, the elements of $S^1(X)$ are the *primes*. The quasi-centre of $G(X)$ is a free abelian group, the structure group of a self-adjoint L^*-algebra $X_0 \sqcup \{1\}$. If $x_0 < x$ with $x_0 \in X_0$ and $x \in S^1(X)$, then $x_0 = x^*x$, and the same holds for any other prime $y \in X$ “above” x_0, so that $x^*x = y^*y$ (“recombination”). For distinct primes $x_0, y_0 \in X_0$ with $x_0 < x \in S^1(X)$ and $y_0 < y \in S^1(X)$, there are unique $x', y' \in S^1(X)$ with $x_0 < x'$ and $y_0 < y'$ such that $xy = y'x'$ (“metacommutation”). Note that for an L^*-algebra, there is no trouble with units.

For the ring H of Hurwitz quaternions, we show first that the primes with odd norm, normalized with respect to units and together with 1, form a discrete L^*-algebra X_H^* which generates a subgroup G_H^* of $\mathbb{H}^\times$ isomorphic to the structure group $G(X_H^*)$, a noetherian modular right ℓ-group (Theorem 2). The quasi-centre and the centre are determined explicitly (Corollary 3). Then we extend the L^*-algebra X_H^* to the full L^*-algebra X_H, with a pair of primes ζ, ζ^* instead of the ramified Hurwitz prime over 2, which has to be taken as a “double point” (Theorem 3). This extends metacommutation to all Hurwitz primes, with the speciality that the structure group $G(X_H)$ no longer embeds into $\mathbb{H}^\times$. For any integer $n > 1$, the Hurwitz prime divisors of n generate a Garside group.

In the last section, we give some examples and methods for explicit calculation. In particular, we give a simple combinatorial scheme to enumerate the $p+1$ normalized Hurwitz primes over any rational prime p. The cycle structure of the metacommutation maps is determined. An example shows that the cycle structure of these permutations, in contrast to the sign $\left(\frac{q}{p}\right)$, depends on the reduced trace of the acting prime.

1. *L*-algebras and their structure group

L-algebras were introduced in [29]. They are based on the cycloid equation [30]

$$(x \to y) \to (x \to z) = (y \to x) \to (y \to z) \tag{1}$$

which first occurred in algebraic logic [3,18,36]. It can also be found in the theory of Garside groups [11] and ℓ-groups [29], in connection with certain solutions of the quantum Yang–Baxter equation [28,31], and in the theory of von Neumann algebras and orthomodular lattices [34].

Let X be a set with a binary operation $\rightarrow$. An element $1 \in X$ is said to be a *logical unit* [29] if

$$x \rightarrow x = x \rightarrow 1 = 1\,; \quad 1 \rightarrow x = x$$

holds for all $x \in X$. If X has a logical unit and satisfies Eq. (1) such that the implication

$$x \rightarrow y = y \rightarrow x = 1 \implies x = y \tag{2}$$

is valid for $x, y \in X$, then X is said to be an *L-algebra* [29]. Any L-algebra X is equipped with a partial order

$$x \leqslant y \iff x \rightarrow y = 1. \tag{3}$$

An L-algebra X is said to be *self-similar* [29] if the maps $y \mapsto (x \rightarrow y)$ are bijections from $\{y \in X \mid y \leqslant x\}$ onto X. Thus, for a self-similar L-algebra X, any $z \in X$ is of the form $z = x \rightarrow y$ for a unique element $y \leqslant x$. We write $y = zx$. By [29], Theorem 1, this multiplication makes X into a monoid, and the monoid structure determines the self-similar L-algebra. Precisely, a self-similar L-algebras is characterized by the equations

$$x = y \rightarrow xy \tag{4}$$

$$xy \rightarrow z = x \rightarrow (y \rightarrow z) \tag{5}$$

$$(x \rightarrow y)x = (y \rightarrow x)y. \tag{6}$$

With respect to the partial order (3), X is a $\wedge$-semilattice with meet given by Eq. (6):

$$x \wedge y = (x \rightarrow y)x.$$

Every L-algebra X has a *self-similar closure* $S(X)$, that is, an embedding $X \hookrightarrow S(X)$ into a self-similar L-algebra $S(X)$, generated by X as a monoid. By [29], Theorem 3, the self-similar closure is unique, up to isomorphism. Note that Eq. (6) implies the left Ore condition, while Eq. (4) shows that self-similar L-algebras are right cancellative. Thus $S(X)$ has a left group of fractions $G(X)$, with a natural map

$$q\colon X \hookrightarrow S(X) \longrightarrow G(X).$$

We call $G(X)$ the *structure group* of X. There are special cases where the monoid homomorphism $S(X) \rightarrow G(X)$ is injective (see [29], Theorem 4; [32], Theorem 3; [34], Theorem 2). In the next section, we give another example where this happens.

Definition 1. We define an *L^*-algebra* to be an L-algebra X with an involution $x \mapsto x^*$ such that $1^* = 1$ and the following are satisfied for $x, y \in X$:

$$x^* \leqslant x \to (y \to x) \tag{7}$$

$$y \leqslant x^* \to (x \to y) \tag{8}$$

Recall that an L-algebra X is said to be *discrete* [32] if the elements of $S^1(X) := X \setminus \{1\}$ are pairwise incomparable. By [32], Proposition 18, discrete L-algebras are equivalent to geometric lattices with a certain labelling. In particular, $S(X)$ is a lower semimodular lattice and has a grading

$$S(X) = \bigsqcup_{n \in \mathbb{N}} S^n(X)$$

with $S^n(X) := \{x_1 \cdots x_n \mid x_1, \ldots, x_n \in S^1(X)\}$. If X is a discrete L^*-algebra, the inequality (8) shows that for any $x \in S^1(X)$, the sets

$$C(x) := \{y \in S^1(X) \mid x^* \leqslant x \to y\}, \qquad C'(x) := \{y \in S^1(X) \mid y = x^* \to (x \to y)\}$$

form a partition $S^1(X) = C(x) \sqcup C'(x)$ with $x \in C(x)$.

Definition 2. Let X be a discrete L^*-algebra. We call a subset $Y \subset S^1(X)$ *invariant* if Y is closed with respect to the involution $y \mapsto y^*$ and $x \to y \in Y \cup \{1\}$ holds for all $x \in X$ and $y \in Y$.

Thus any invariant subset $Y \subset S^1(X)$ gives rise to an L^*-subalgebra $Y \cup \{1\}$ of X.

Proposition 1. *Let X be a discrete L^*-algebra. The $C(x)$ are invariant subsets of $S^1(X)$ which satisfy*

$$y \in C(x) \implies C(y) = C(x)$$

for all $x, y \in S^1(X)$. For any $x \in S^1(X)$, the map $y \mapsto (x \to y)$ is bijective on $C'(x)$.

Proof. Suppose that $x^* \nleqslant x \to x^*$ holds for some $x \in X$. Then $x \neq 1$, and (7) implies that $x = x^* \to (x \to x^*)$. Hence (8) gives $x^* = x$, contrary to our assumption. Thus

$$x^* \leqslant x \to x^* \tag{9}$$

for all $x \in X$. We show first that $C(x^*) = C(x)$ holds for all $x \in S^1(X)$. So we have to verify

$$x^* \leqslant x \to y \implies x \leqslant x^* \to y$$

for all $x, y \in S^1(X)$. By (9), we can assume that x, x^*, and y are distinct. Then $x^* \leqslant x \to y$ implies that $x^* = x \to y$, which yields $1 = x^* \to (x \to x^*) = (x \to y) \to (x \to x^*) = (y \to x) \to (y \to x^*)$. Hence $y \to x \leqslant y \to x^*$, and thus $y \to x = y \to x^*$. So we obtain $(x^* \to y) \to (x^* \to x) = (y \to x^*) \to (y \to x) = 1$, which implies that $x = x^* \to x = x^* \to y$.

For $x, y \in S^1(X)$ with $y \in C(x)$, we have $x^* \leqslant x \to y$. Hence $x^* \leqslant x \to x^* \leqslant x \to (x \to y)$, which yields $x \to y \in C(x)$. On the other hand, $y \in C'(x)$ implies that $x \to \bigl(x^* \to (x \to y)\bigr) = x \to y$, which yields $x \to y \in C'(x^*)$. Since $C(x^*) = C(x)$, we also have $C'(x^*) = C'(x)$. Thus $x \to y \in C'(x)$. The definition of $C'(x) = C'(x^*)$ shows that the map $y \mapsto (x \to y)$ is bijective on $C'(x)$, with inverse $y \mapsto (x^* \to y)$.

Now let $x, y \in S^1(X)$ with $y \in C(x) \setminus \{x\}$ be given. For any $z \in C(x) \setminus \{y\}$ this implies that $1 = x^* \to x^* = (x \to y) \to x^* \leqslant (x \to y) \to (x \to z) = (y \to x) \to (y \to z)$. Hence $y \to x \leqslant y \to z$, and thus

$$\forall\, z \in C(x) \setminus \{y\} \colon y \to x = y \to z.$$

Suppose that $x \in C'(y)$. Then $y \to z = y \to x \in C'(y)$, which implies that $z \in C'(y)$. Hence $x = z$, and therefore, $C(x) = \{x, y\}$. Since $C(x^*) = C(x)$, this gives $x^* \neq y$. So we get $x = x^* = x \to y$. By (7), this yields $y^* \leqslant y \to (x \to y) = y \to x$. Hence $y \to x = y^* \in C(y)$, a contradiction. So we have $x \in C(y)$. Consequently, $y^* \leqslant y \to x = y \to z$ for all $z \in C(x) \setminus \{y\}$, which proves that $C(x) \setminus \{y\} \subset C(y)$. Thus $C(x) \subset C(y)$ for all $y \in C(x)$. By symmetry, this shows that $C(y) = C(x)$. Therefore, (7) and (9) imply that the $C(x)$ are invariant. □

Remark. The preceding proof shows that (7) can almost be replaced by (9). Namely, if $x, y \in S^1(X)$ satisfy $y \in C(x)$ and $x \notin C(y)$, then $C(x) = \{x, y\}$ and $x = x^*$. If (7) holds, we have seen that such a configuration is impossible.

Corollary. *Let X be a discrete L^*-algebra. For $x, y \in X$,*

$$x \to y = y \to x \implies x = y.$$

Proof. Suppose that $x \neq y$ and $x \to y = y \to x$. Then $x, y \in S^1(X)$ and $C(x) = C(y)$. Hence $x^* = x \to y = y \to x = y^*$, contrary to $x \neq y$. □

By Proposition 1, the $C(x)$ of a discrete L^*-algebra X give rise to L^*-subalgebras $\widetilde{C}(x) := C(x) \sqcup \{1\}$, the *components* of X. The *reduced components* $C(x)$ form a partition

$$S^1(X) = \bigsqcup_{x \in \Delta} C(x),$$

with a representative system Δ for the $C(x)$. Being invariant under $y \mapsto (z \to y)$, the components act on each other, and any union of components is an L^*-subalgebra of X.

The whole structure of X is given by the mutual action of the components. This will give the abstract basis for *metacommutation* in the next section.

The structure of a single component is very simple. Such an L^*-algebra $\widetilde{C}(x)$ will be called *irreducible.* For $x, y \in S^1(X)$, we have

$$x \to y = \begin{cases} 1 & \text{for } x = y \\ x^* & \text{for } x \neq y. \end{cases} \tag{10}$$

So all what matters is "metacommutation", the mutual action between the components, and the coherence condition (1) for triples of components. The next result characterizes discrete L^*-algebras with two components.

Proposition 2. *Let X be a set with a partition $X = X_1 \sqcup X_2$ into non-empty subsets, invariant under an involution $x \mapsto x^*$ of X. Let $\to$ be a binary operation on $\widetilde{X} := X \sqcup \{1\}$ with logical unit 1 satisfying Eq. (10) for the X_i. Assume that $x_i \to x_j \in X_j$ holds for $x_i \in X_i$, $x_j \in X_j$, and $i \neq j$, with permutations $x_j \mapsto (x_i \to x_j)$. Then $\widetilde{X}$ is a discrete L^*-algebra with reduced components X_i if and only if for $x_i \in X_i$ and $i \neq j$,*

$$x_j = x_i^* \to (x_i \to x_j) \tag{11}$$

$$(x_i \to x_j)^* = (x_j \to x_i) \to x_j^*. \tag{12}$$

Proof. It is easily checked that Eq. (10) makes any component into an L^*-algebra. Unless the variables x, y, z in Eq. (1) are all distinct and $\neq 1$, Eq. (1) reduces to the properties of 1 as a logical unit. So we can assume that x, y, z are distinct and in X. Up to symmetry, there are just two possibilities for x, y, z. Either $x, y \in X_1$ and $z \in X_2$, or $x \in X_1$ and $y, z \in X_2$. The first case then states that the right-hand side of Eq. (11) does not depend on x_i, while the second case gives Eq. (12). If $\widetilde{X}$ is an L^*-algebra, Eq. (11) follows by (8). Conversely, (7) and (8) easily follow by Eqs. (10) and (11). □

Corollary 1. *Let X be a discrete L^*-algebra. The map $(x, y) \mapsto \big((x \to y)^*, (y \to x)^*\big)$ is an involution on $X \times X$ outside the diagonal.*

Proof. If $x, y \in X$ belong to distinct components, Eq. (12) gives

$$(x \to y)^* \to (y \to x)^* = x^*,$$

which proves the claim for this case. Thus, assume that x and y belong to the same component, and $x \neq y$. Then Eq. (10) shows that $(x \to y)^* = x^{**} = x$. So the map is identical in this case. □

Corollary 2. *The involution $x \mapsto x^*$ of a discrete L^*-algebra X admits a unique extension to an anti-automorphism of $S(X)$ as a monoid.*

Proof. We show first that the implication

$$xy = zt \implies y^*x^* = t^*z^* \tag{13}$$

holds for $x, y, z, t \in S^1(X)$. For $y = t$, we have $x = z$, and there is nothing to prove. So we assume that $xy = zt$ and $y \neq t$. Then $x = y \to xy = y \to zt \leqslant y \to t$. Since $y \neq t$, this yields $x = y \to t$. Hence $(t \to y)t = (y \to t)y = xy = zt$, and thus $t \to y = z$. If $C(y) = C(t)$, we infer that $x = y^*$ and $z = t^*$, and (13) follows immediately. Thus, assume that $C(y) \neq C(t)$. Then Eq. (12) gives $x^* = (y \to t)^* = (t \to y) \to t^* = z \to t^*$. By Eq. (11), this implies that $t^* = z^* \to x^*$. Similarly, $y^* = x^* \to z^*$. Hence Eq. (6) yields $y^*x^* = (x^* \to z^*)x^* = (z^* \to x^*)z^* = t^*z^*$, which proves (13). Thus $(xy)^*$ can be defined unambiguously to be $(xy)^* := y^*x^*$.

Now we extend (13) and the definition of $(xy)^*$ inductively to $x, z \in S^n(X)$ for all $n \in \mathbb{N}$. Assume that this has been done for $n \leqslant m$, and let $a, b \in S^m(X)$ and $x, y \in S^1(X)$ with $ax = by$ be given. We have to verify $x^*a^* = y^*b^*$.

Since $a \leqslant x \to by \leqslant x \to y$, we have $ax = \big(a \wedge (x \to y)\big)x = \big((x \to y) \to a\big)(x \to y)x$. Similarly, $by = \big((y \to x) \to b\big)(y \to x)y$. Therefore, $(x \to y)x = (y \to x)y$ implies that $(x \to y) \to a = (y \to x) \to b =: c$. Thus $a = c(x \to y)$ and $b = c(y \to x)$. The inductive hypothesis gives $a^* = (x \to y)^*c^*$ and $b^* = (y \to x)^*c^*$. Hence $x^*a^* = x^*(x \to y)^*c^* = ((x \to y)x)^*c^* = (x \wedge y)^*c^*$. By symmetry, this proves the claim. For $x_1, \ldots, x_n \in S^1(X)$, we obtain $(x_1 \cdots x_n)^* = x_n^* \cdots x_1^*$, which yields $(ab)^* = b^*a^*$ for all $a, b \in S(X)$. □

2. Metacommutation for discrete L^*-algebras

Recall that a group G with a lattice order is said to be a *right ℓ-group* [32] if the right multiplications are lattice automorphisms, that is,

$$a \leqslant b \implies ac \leqslant bc$$

holds for all $a, b, c \in G$. Of course, this implies that $(a \vee b)c = ac \vee bc$ and $(a \wedge b)c = ac \wedge bc$. The set

$$G^- := \{a \in G \mid a \leqslant 1\}$$

is called the *negative cone* of G. By [32], Theorem 1, the negative cone of a right ℓ-group G is a self-similar L-algebra with

$$a \to b = ba^{-1} \wedge 1.$$

Theorem 1. *Let X be a discrete L^*-algebra. Then $G(X)$ is a right ℓ-group, and $S(X)$ is an L^*-algebra which can be identified with the negative cone of $G(X)$. The underlying lattice of $G(X)$ is modular.*

Proof. To show that $S(X)$ is a modular lattice, we apply [32], Proposition 19. For $x, y, u, v \in S^1(X)$ with $x \neq y$ and $(x \to y) \to u = (y \to x) \to v$ we have to find an element $z \in S(X)$ with $x \to z = u$ and $y \to z = v$. (We use the opportunity to correct an inaccuracy: [32], Proposition 19, has $z \in X$ instead of $z \in S(X)$. Alternatively, one could replace $(x \to y) \to u = (y \to x) \to v$ by $(x \to y) \to u = (y \to x) \to v < 1$.)

Case 1: $C(x) = C(y)$. Then $x^* \to u = y^* \to v$. If $x^* = u$, then $y^* = v$, and $z := x \wedge y$ satisfies $x \to z = u$ and $y \to z = v$. Thus, by symmetry, we can assume that $x^* \neq u$ and $y^* \neq v$. Suppose that $C(x) = C(u)$. Then $x = x^* \to u = y^* \to v$, which yields $v \leqslant y \to (y^* \to v) = y \to x = y^*$, a contradiction. Thus $C(u) \neq C(x) = C(y) \neq C(v)$. Then $z := x^* \to u = y^* \to v$ meets the requirement.

Case 2: $C(x) \neq C(y)$. Assume first that $C(u) = C(y)$. If $u = x \to y$, we obtain $y \to x = v$, and we can choose $z := x \wedge y$. So let us assume that $u \neq x \to y$ and $v \neq y \to x$. By Proposition 2, we have $(y \to x) \to y^* = (x \to y)^* = (x \to y) \to u = (y \to x) \to v$. If $C(v) = C(x)$, then $(x \to y)^* = (y \to x)^*$, which yields $x = y$ by the corollary of Proposition 1. Thus $C(v) \neq C(x)$, which yields $y^* = v$ by virtue of Proposition 2. Whence $z := x^* \to u$ satisfies $x \to z = u$ and $y \to z = y \to (x^* \to u) = y^* = v$.

Next assume that $C(u) \neq C(y)$ and $C(v) \neq C(x)$. Then

$$\begin{aligned} u &= (x \to y)^* \to \big((y \to x) \to v\big) = \big((y \to x) \to y^*\big) \to \big((y \to x) \to v\big) \\ &= \big(y^* \to (y \to x)\big) \to (y^* \to v) = x \to (y^* \to v). \end{aligned}$$

So $C(u) = C(v)$, and we can choose $z := x^* \to u = y^* \to v$. Thus $S(X)$ is modular.

By the corollary of Proposition 1 and Corollary 1 of Proposition 2, X is non-degenerate in the sense of [32], Definition 11. Therefore, [32], Theorems 1 and 4 imply that $S(X)$ is the negative cone of a modular right ℓ-group G. So $G \cong G(X)$.

It remains to verify that $S(X)$ is an L^*-algebra. For $x, y \in S^1(X)$ with $C(x) \neq C(y)$, let $y \mapsto x^y$ be the inverse of the map $y \mapsto (x \to y)$. Furthermore, we set

$$^{x}y := x^y \to y$$

for $C(x) \neq C(y)$. The substitution $x \mapsto x^y$ in Eq. (6) then gives

$$xy = {}^{x}y \cdot x^y. \tag{14}$$

Furthermore, ${}^{y\to x}y = (y \to x)^y \to y = x \to y$. So Proposition 2 gives ${}^{(y\to x)^*}\big({}^{y\to x}y\big) = \big((y \to x)^*\big)^{x\to y} \to (x \to y) = \big((x \to y)^* \to (y \to x)^*\big) \to (x \to y) = x^* \to (x \to y) = y$. Thus

$${}^{x^*}\big({}^{x}y\big) = y.$$

For $x, y \in S^1(X)$ with $C(x) = C(y)$, Eq. (6) gives

$$x^*x = y^*y. \tag{15}$$

Next we show that the elements x^*x with $x \in S^1(X)$ commute with all $y \in S^1(X)$. If $C(x) = C(y)$, this follows by Eq. (15). So let us assume that $C(x) \neq C(y)$. By Proposition 2 and Eqs. (14) and (15), we have

$$\begin{aligned} yx^*x &= {}^{y}x^* \cdot y^{x^*} \cdot x = (y^{x^*} \to x^*) \cdot (x \to y)x = \big((x \to y) \to x^*\big)(y \to x)y \\ &= (y \to x)^*(y \to x)y = x^*xy. \end{aligned}$$

Thus x^*x commutes with every element of $S(X)$. More generally,

$$a^*a \cdot b = b \cdot a^*a \tag{16}$$

holds for all $a, b \in S(X)$. Assume that this has been verified for some $a \in S(X)$. For any $x \in S^1(X)$, this implies that $(xa)^*(xa)b = a^*x^*xab = a^*abx^*x = ba^*ax^*x = ba^*x^*xa = b(xa)^*(xa)$. By induction, this proves Eq. (16). Now (7) and (8) follow immediately for all $a, b \in S(X)$. □

For a right ℓ-group G, an element $a \in G$ is said to be *normal* [32] if

$$b \leqslant c \iff ab \leqslant ac$$

holds for all $b, c \in G$. The set $N(G)$ of normal elements of G is called the *quasi-centre* of G. The centre of G will be denoted by $Z(G)$. By [33], Proposition 5, $N(G)$ is an ℓ-group.

Corollary 1. *Let X be a discrete L^*-algebra. The quasi-centre of $G(X)$ is a free abelian group, generated by the elements x^*x with $x \in S^1(X)$ and $x \nleqslant y \to x$ for some $y \in X$, and the elements $x \in S^1(X)$ with $x \leqslant y \to x$ for all $y \in X$. In the latter case, $C(x) = \{x, x^*\}$ and $xyx^{-1} = x \to y$ for all $y \in C'(x)$.*

Proof. By Eq. (16), $a^*a \in Z(G(X))$ for all $a \in S(X)$. Since $N(G(X))$ is an ℓ-group, Birkhoff's theorem [2] implies that $N(G(X))$ is free abelian. Let $a \in N(G(X))$ be maximal with $a < 1$. Then $a \leqslant x$ for some $x \in S^1(X)$. Assume first that $x \leqslant y \to x$ for all $y \in X$. Then $C(x) = \{x, x^*\}$, and Eq. (14) gives $xy = {}^{x}y \cdot x^y = (x^y \to y)x = (x \to y)x$ for all $y \in C'(x)$. Hence $xyx^{-1} = x \to y$, and $x^{-1}yx = y^x$. So the negative cone of $G(X)$ is invariant under conjugation with x, which shows that x is normal, and $a = x$. Otherwise, there is an element $y \in X$ with $x \nleqslant y \to x$. Then $ay \leqslant a \leqslant x$ implies that $a \leqslant y \to x$. By Eq. (15), this yields $a \leqslant x \wedge (y \to x) = x^*x$. Since x^*x is normal, $a = x^*x$. □

Remark. Corollary 1 shows that the structure group of a discrete L^*-algebra X can be regarded as a generalized *Garside group* [13,11,12] in the sense that instead of a single Garside element, there are *enough* normal elements, so that every element of $G(X)$ is majorized by a normal element. By Corollary 1, we have the following

Corollary 2. *Let X be a discrete L^*-algebra. Then $x \in S^1(X)$ is central in $G(X)$ if and only if $x \leqslant y \to x$ and $y \leqslant x \to y$ for all $y \in X$. The centre of $G(X)$ is a free abelian group, generated by the $x \in S^1(X) \cap Z(G(X))$ and the elements x^*x with $x \in S^1(X) \setminus Z(G(X))$.*

The next corollary shows that the operation → of an L^*-algebra generalizes meta-commutation of Hurwitz primes:

Corollary 3. *Let X be a discrete L^*-algebra. For any $x, y \in S^1(X)$ with $C(x) \neq C(y)$, there is a unique pair of elements ${}^xy \in C(y)$ and $x^y \in C(x)$ with $xy = {}^xy \cdot x^y$.*

Proof. The existence follows by Eq. (14). To verify uniqueness, assume that $xy = x'y'$ holds for some $x' \in C(x)$ and $y' \in C(y)$. Then $xy \leqslant y'$, which gives $x \leqslant y \to y'$. Since $x \nleqslant y^*$, we obtain $y \leqslant y'$. Whence $y = y'$. □

Example 1. Let $\widetilde{X}$ be the discrete L^*-algebra with two reduced components $X_1 = \{x, x^*\}$ and $X_2 = \{y, y^*\}$, such that the elements of X_1 act non-trivially on X_2, and y, y^* act trivially on X_1. By Proposition 2, it is readily checked that $\widetilde{X}$ is an L^*-algebra. By Corollary 1, the quasi-centre of $\widetilde{X}$ is generated by x, x^*, and y^*y, while Corollary 2 shows that the centre is generated by x^*x and y^*y.

Example 2. Recall that a bounded lattice X with an involutive anti-automorphism $x \mapsto x'$ is said to be *orthomodular* [21,17,20] if $x \wedge x' = 0$ and

$$x \leqslant y \implies x \vee (x' \wedge y) = y$$

holds for all $x, y \in X$. By [34], Theorem 1, orthomodular lattices can be regarded as a special class of L-algebras, with the operation

$$x \to y := (x \wedge y) \vee x'.$$

By Definition 1, every orthomodular lattice X is an L^*-algebra with $x^* := x'$.

The next example shows that Theorem 1 does not extend to non-discrete L^*-algebras.

Example 3. An L-algebra X which satisfies $x \leqslant y \to x$ for all $x, y \in X$ is said to a *KL-algebra* [29]. By [29], Proposition 13, the structure group $G(X)$ of a KL-algebra X is a partially ordered group, and the natural map $q \colon X \to G(X)$ is monotone. For example, every partially ordered set Ω with greatest element 1 is a KL-algebra with $x \to y := y$ for $x \nleqslant y$ in Ω. By [29], Theorem 4, the natural map $q \colon \Omega \to G(\Omega)$ is not injective unless $S^1(\Omega)$ is an antichain.

Let us call an L^*-algebra X *self-adjoint* if $x^* = x$ for all $x \in X$. By Definition 1, every KL-algebra is a self-adjoint L^*-algebra. So the map $q\colon X \to G(X)$ need not be injective for a non-discrete L^*-algebra X.

3. The L^*-algebra of Hurwitz primes

Now we apply the results of Section 2 to Hurwitz quaternions. Let $\mathbb{H} = \mathbb{R}\oplus\mathbb{R}i\oplus\mathbb{R}j\oplus\mathbb{R}k$ be the skew-field of quaternions with its subring

$$H := \mathbb{Z}\varrho \oplus \mathbb{Z}i \oplus \mathbb{Z}j \oplus \mathbb{Z}k$$

of *Hurwitz quaternions* [19], where

$$\varrho := \frac{1}{2}(1 + i + j + k).$$

Thus H is a maximal order in $\mathbb{Q}H$ (see [27]). The reduced norm [27] of an element $\alpha = t + xi + yj + zk \in H$ is given by

$$N(\alpha) = \alpha\overline{\alpha} = t^2 + x^2 + y^2 + z^2,$$

where $\overline{\alpha} := t - xi - yj - zk$. Hurwitz [19] proved that H is a left and right principal ideal domain, and he determined its unit group

$$H^\times = \{\pm 1, \pm i, \pm j, \pm k, \frac{1}{2}(\pm 1 \pm i \pm j \pm k)\}$$

of order 24. An element $\varepsilon \in H$ is a unit if and only if $N(\varepsilon) = 1$, and $\pi \in H$ is prime if and only if $N(\pi)$ is a rational prime. This prime number $p := N(\pi)$ is a multiple of π, which is also expressed by saying that π is *lying over* p. Conway and Smith [8] have shown that factorization into primes in H is unique up to three phenomena. The first, obvious one, is *migration of units* between adjacent factors. Secondly, the primes over the same rational prime p come in conjugate pairs. If π and σ are lying over p, then $\pi\overline{\pi} = \sigma\overline{\sigma}$, and the passage from $\pi\overline{\pi}$ to $\sigma\overline{\sigma}$ is called *recombination*. The third phenomenon — *meta-commutation* — is the most interesting one. It states that any pair of primes $\pi, \sigma \in H$, lying over distinct odd rational primes, satisfies $\pi\sigma = \sigma'\pi'$ for a unique pair of primes $\pi', \sigma' \in H$ with $N(\pi) = N(\pi')$ and $N(\sigma) = N(\sigma')$, up to migration of units.

The equation $\pi\sigma = \sigma'\pi'$ can be interpreted as follows. It says that modulo $p := N(\pi)$, right multiplication by σ maps the left ideal $H\pi$ to $H\pi'$. Hurwitz [19] already proved

$$H/pH \cong \mathrm{M}_2(\mathbb{F}_p)$$

for odd p. So H/pH is a semisimple left H-module of length two. Since $\mathrm{M}_2(\mathbb{F}_p)$ is Morita equivalent to $\mathbb{F}_p$, there are exactly $p+1$ left ideals $H\pi$ with $Hp \subsetneq H\pi \subsetneq H$, according to the points of the projective line $\mathbb{P}^1(\mathbb{F}_p)$. Let $\Pi(p)$ denote the set of these left ideals. As right multiplication by σ is linear, it induces an automorphism φ_p^σ of $\mathbb{P}^1(\mathbb{F}_p)$ which gives rise to a permutation Φ_p^σ on $\Pi(p)$. The following result is due to Cohn and Kumar [7].

Proposition 3. *For distinct odd primes $p, q \in \mathbb{Z}$ and a prime $\sigma \in H$ over q, the sign of the permutation Φ_p^σ is given by the Legendre symbol $\left(\frac{q}{p}\right)$.*

This follows by the commutative diagram

$$\begin{tikzcd}
\mathrm{GL}_2(\mathbb{F}_p) \arrow[r, two heads, "\det"] \arrow[d, "\mathrm{sgn}"] & \mathbb{F}_p^\times \arrow[d, "\left(\frac{-}{p}\right)"] \\
\mathrm{C}_2 \arrow[r, equal] & \mathbb{F}_p^\times/(\mathbb{F}_p^\times)^2
\end{tikzcd}$$

since $\det \varphi_p^\sigma = N(\sigma) = q$ (see [16] for a detailed argument).

To get rid of the unit factors of Hurwitz primes, we modify Hurwitz' concept of primary quaternions. With $\zeta := i + j$, we have $\zeta^2 = -2$. Hurwitz [19] proved that half of the units in $H^\times$ can be embedded into $H/2H = H/\zeta^2 H$. In modern language, he found that $H/2H$ is a local algebra with radical $\zeta H/2H$ and $H/\zeta H \cong \mathbb{F}_4$. (Note that $\zeta H = H\zeta$.)

Now consider the local ring $H/\zeta^3 H$. Its unit group has $|H/\zeta^3 H| - |\mathrm{Rad}(H/\zeta^3 H)| = 64 - 16 = 48$ elements. We show that

$$(H/\zeta^3 H)^\times \cong H^\times \times \langle i + j + k \rangle, \tag{17}$$

where $\langle i+j+k \rangle$ is of order 2 in $(H/\zeta^3 H)^\times$ since $(i+j+k)^2 = -3 = 1-\zeta^4$. Furthermore, $H^\times$ embeds into $H/\zeta^3 H$, and $i+j+k = 2\varrho - 1$ commutes with ϱ, i, j, k modulo ζ^3. Indeed, $i(i + j + k) - (i + j + k)i = 2(k - j) = \zeta^3(\varrho - 1 - i)$. By symmetry, this proves (17).

Definition 3. We call $\alpha \in H \smallsetminus H\zeta$ *monic* if $\alpha - (i + j + k)^s \in \zeta^3 H$ for some $s \in \{0, 1\}$.

With $1 + 2\varrho$ instead of $i + j + k$, Hurwitz calls such elements $\alpha \in H$ “primary”. Our terminology is motivated by the concept of monic polynomial, representing a polynomial up to units. Note that for monic $\alpha := a + bi + cj + dk \in H$, the coefficients a, b, c, d belong to $\mathbb{Z}$. By Definition 3, the set S_H^* of monic elements $\alpha \in H \smallsetminus H\zeta$ is a submonoid of $H \smallsetminus \{0\}$. The ramified prime ζ plays a particular part. A simple calculation gives

$$\zeta(a + bi + cj + dk)\zeta^{-1} = a + ci + bj - dk.$$

Hence $\zeta(i + j + k)\zeta^{-1} = -(i + j + k) - \zeta^3$. Let us write X_H^* for the set of monic primes in $H \smallsetminus H\zeta$. Note that S_H^* is not closed under conjugation $\alpha \mapsto \overline{\alpha}$. Define

$$\alpha^* := \begin{cases} \overline{\alpha} & \text{for } \overline{\alpha} \in S_H^* \\ -\overline{\alpha} & \text{for } \overline{\alpha} \notin S_H^* \end{cases} \tag{18}$$

for $\alpha \in S_H^*$, and $\zeta^* := -\zeta$. Thus $\alpha \mapsto \alpha^*$ is an involution of S_H^* which satisfies

$$(\alpha\beta)^* = \beta^*\alpha^*.$$

The ramified prime ζ comes as a pair $\pm\zeta$ of associated primes, a "double point" in the full set $X_H := X_H^* \cup \{\pm\zeta\}$ of Hurwitz primes. For monic primes of H, the sign in (18) can be determined explicitly:

Proposition 4. *For $\pi \in X_H$ with $p := N(\pi)$, we have $\pi^* = \left(\frac{-1}{p}\right)\overline{\pi}$. If p is odd, $\pi - 1 \in \zeta^3 H$ if and only if $\left(\frac{-1}{p}\right) = 1$.*

Proof. We can assume that p is odd. If $\pi - 1 \in \zeta^3 H$, then $\overline{\pi} \in X_H^*$ and $\overline{\pi} - 1 \in \zeta^3 H$, which yields $p - 1 = \pi\overline{\pi} - 1 \in \zeta^3 H \cap \mathbb{Z} = 4\mathbb{Z}$. Otherwise, $\pi - (i + j + k) \in \zeta^3 H$, which implies that $\overline{\pi} \notin X_H$ and $p - 3 \in \zeta^3 H \cap \mathbb{Z} = 4\mathbb{Z}$. So the sign in (18) with $\alpha = \pi$ is given by the Legendre symbol $\left(\frac{-1}{p}\right)$. □

In particular, if p is an odd rational prime, $p^* := \left(\frac{-1}{p}\right)p \in S_H^*$. Thus, for an odd integer $n > 0$, either $n \in S_H^*$ or $-n \in S_H^*$. Let G_H^* be the subgroup of $\mathbb{H}^\times$ generated by S_H^*. Then any element of G_H^* is of the form $\frac{1}{n}\alpha$ with $\alpha \in S_H^*$ and $n \in S_H^* \cap \mathbb{Z}$. We endow G_H^* with the partial order

$$\alpha \leqslant \beta \;:\Longleftrightarrow\; \exists\, \gamma \in S_H^* \colon \alpha = \gamma\beta \;\Longleftrightarrow\; H\alpha \subset H\beta. \tag{19}$$

To state our second main theorem, we adjoin a greatest element 1 to X_H to obtain the subsets

$$\widetilde{X}_H := X_H \cup \{1\}, \qquad \widetilde{X}_H^* := X_H^* \cup \{1\} \tag{20}$$

of H, where 1 stands for the "infinite Hurwitz prime".

Theorem 2. *The subset $\widetilde{X}_H^*$ of S_H^* is a discrete L^*-algebra with structure group G_H^* such that $S_H^* = (G_H^*)^-$.*

Proof. Since H is a left principal ideal domain, the partial order (19) makes G_H^* into a modular lattice. Thus G_H^* is a right ℓ-group with $S_H^* = (G_H^*)^-$, and X_H^* consists of the coatoms of S_H^*. By [32], Theorem 1, the negative cone S_H^* is a self-similar L-algebra with

$$\alpha \to \beta := \beta\alpha^{-1} \wedge 1 \tag{21}$$

such that $\alpha \leqslant \beta \Longleftrightarrow \alpha \to \beta = 1$. By [32], Proposition 5, the modularity of the lattice G_H^* implies that X_H^* is closed with respect to the operation (21). Hence $\widetilde{X}_H^*$ is an L-algebra with self-similar closure S_H^*, and G_H^* is the structure group of $\widetilde{X}_H^*$. Since $\pi^*\pi$ is central for all $\pi \in X_H^*$, the inequalities (7) and (8) hold in $\widetilde{X}_H^*$. Thus $\widetilde{X}_H^*$ is an L^*-algebra. □

By Corollary 3 of Theorem 1, we infer that metacommutation of Hurwitz primes is a quantum phenomenon which can be explained by the L^*-algebra structure of $\widetilde{X}_H^*$:

Corollary 1. *For any pair $\pi, \sigma \in X_H^*$ with $N(\pi) \neq N(\sigma)$ there are unique primes ${}^{\pi}\sigma$ and π^{σ} in X_H^* with $N(\pi^{\sigma}) = N(\pi)$ and $N({}^{\pi}\sigma) = N(\sigma)$ such that*

$$\pi \cdot \sigma = {}^{\pi}\sigma \cdot \pi^{\sigma}. \tag{22}$$

Corollary 2. *The operation in the L^*-algebra $\widetilde{X}_H^*$ is given by*

$$\pi \to \sigma := \begin{cases} 1 & \text{for } \pi = \sigma \\ \pi^* & \text{for } N(\pi) = N(\sigma) \text{ and } \pi \neq \sigma \\ \sigma^{\pi^*} & \text{for } N(\pi) \neq N(\sigma). \end{cases}$$

This follows immediately by Proposition 2. Theorem 1 with its Corollary 1 give

Corollary 3. *The structure group G_H^* is a noetherian modular right ℓ-group. The quasi-centre of G_H^* satisfies $N(G_H^*) = G_H^* \cap \mathbb{Q} = Z(G_H^*)$.*

Now we show the L^*-algebra structure of X_H^* naturally extends to X_H to cover the "double point" $\pm\zeta \in X_H$ which cannot be handled appropriately within $\mathbb{H}^\times$. For $\pi \in X_H^*$ with $N(\pi) = p$ we define $\zeta \to \zeta^* := \zeta^*$ and $\zeta^* \to \zeta := \zeta$, and

$$\zeta \to \pi := \left(\tfrac{-1}{p}\right)\zeta\pi\zeta^{-1}, \qquad \pi \to \zeta := \left(\tfrac{-1}{p}\right)\zeta. \tag{23}$$

Hence $\zeta^* \to \pi = \left(\frac{-1}{p}\right)\zeta^{-1}\pi\zeta = \zeta \to \pi$ and $\pi \to \zeta^* = \left(\frac{-1}{p}\right)\zeta^*$. Let $\mathbb{Q}^*$ denote the subgroup of $\mathbb{Q}^\times$ generated by 2 and all p^* for odd rational primes p. Thus $\mathbb{Q}^*$ is of index 2 in $\mathbb{Q}^\times$.

Theorem 3. *With Eqs. (23), X_H is a discrete L^*-algebra with quasi-centre $N(G(X_H)) = Z(G(X_H)) \cong \mathbb{Q}^*$.*

Proof. Let $\pi, \sigma \in X_H^*$ be given. Up to sign, conjugation with ζ is a lattice automorphism of S_H^*. So we have $(\zeta \to \pi) \wedge (\zeta \to \sigma) = \pm\zeta(\pi \wedge \sigma)\zeta^{-1}$. Hence

$$\big((\zeta \to \pi) \to (\zeta \to \sigma)\big)(\zeta \to \pi) = \pm\zeta(\pi \to \sigma)\zeta^{-1} \cdot \zeta\pi\zeta^{-1} = \big(\zeta \to (\pi \to \sigma)\big)(\zeta \to \pi).$$

Multiplying from the right with $(\zeta \to \pi)^{-1}$ gives

$$(\zeta \to \pi) \to (\zeta \to \sigma) = (\pi \to \zeta) \to (\pi \to \sigma).$$

The same holds if ζ is replaced by ζ^*. For $\pi, \sigma \in X_H^*$ with $N(\pi) = p$ and $N(\sigma) = q$, we have $(\pi \to \sigma) \to (\pi \to \zeta) = \left(\frac{-1}{p}\right)\left(\frac{-1}{q}\right)\zeta = (\sigma \to \pi) \to (\sigma \to \zeta)$, and

$$(\zeta^* \to \pi) \to (\zeta^* \to \zeta) = \left(\tfrac{-1}{p}\right)\zeta = \pi \to \zeta = (\pi \to \zeta^*) \to (\pi \to \zeta).$$

Furthermore, $(\zeta \to \zeta^*) \to (\zeta \to \pi) = \zeta^* \to (\zeta \to \pi) = \pi = (\zeta^* \to \zeta) \to (\zeta^* \to \pi)$, which proves that X_H is an L-algebra. As (7) and (8) trivially hold, X_H is a discrete L^*-algebra. The rest follows by Corollary 1 of Theorem 1. □

Remarks. 1. With the substitution $\pi \mapsto (\sigma \to \pi)$, the metacommutation equation (22) becomes

$$(\sigma \to \pi)\sigma = (\pi \to \sigma)\pi,$$

which coincides with Eq. (6). Note that in contrast to Eq. (22), this equation holds for all $\pi, \sigma \in X_H^*$, without restriction on the norm.

2. In particular, Theorem 3 shows that for any integer $n \in \mathbb{Q}^*$, the primes in X_H which divide n generate a Garside subgroup of $G(X_H)$.

4. The cycles of the metacommutation maps

Let p be an odd rational prime. Choose $a, b \in \mathbb{Z}$ with

$$a^2 + b^2 \equiv -1 \pmod{p}. \tag{24}$$

The matrices

$$i = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad j = \begin{pmatrix} a & b \\ b & -a \end{pmatrix}, \qquad k = \begin{pmatrix} b & -a \\ -a & -b \end{pmatrix}$$

satisfy $i^2 = j^2 = k^2 = ijk = -1$. They give a representation

$$\varrho_p \colon H \twoheadrightarrow \overline{H}_p := \mathrm{M}_2(\mathbb{F}_p) \tag{25}$$

with $\operatorname{Ker} \varrho_p = Hp$. The monic Hurwitz primes $\pi_0, \ldots, \pi_p$ over p correspond to the non-zero proper left ideals $\overline{H}_p \varrho_p(\pi_i)$ of $\overline{H}_p$. For each i, the rows of the matrices in $\overline{H}_p \varrho_p(\pi_i)$ generate a one-dimensional subspace of $\mathbb{F}_p^2$, that is, a point in $\mathbb{P}^1(\mathbb{F}_p)$. Now if σ is a monic Hurwitz prime over an odd rational prime $q \neq p$, then $\pi_i \sigma = {}^{\pi_i}\sigma \cdot \pi_i^{\sigma}$ implies that $H\pi_i \cdot \sigma = H\pi_i^{\sigma} + Hp$. Therefore, the metacommutation map $\pi_i \mapsto \pi_i^{\sigma}$ is given by the standard action of $\varrho_p(\sigma)$ on $\mathbb{P}^1(\mathbb{F}_q)$.

For $p = 3$, the representation (25) induces an isomorphism between the unit group $H^{\times}$ and the binary tetrahedral group $\mathrm{SL}_2(\mathbb{F}_3)$. The representing matrix of an arbitrary Hurwitz quaternion is

$$\varrho_p(t + xi + yj + zk) = \begin{pmatrix} t + ya + zb & x + yb - za \\ -x + yb - za & t - ya - zb \end{pmatrix}.$$

As is well known and easily checked, ϱ_p maps the reduced trace $2t$ of $t + xi + yj + zk$ to the trace of the matrix, and the reduced norm to the determinant.

To determine the $p + 1$ primes $\pi = t + xi + yj + zk$ lying over p, we have to collect the solutions of the equation

$$p = t^2 + x^2 + y^2 + z^2. \tag{26}$$

To study the metacommutation action of π on some $\mathbb{P}^1(\mathbb{F}_q)$, it is enough to know $\pm\pi$. Thus, besides Eq. (26), it suffices to make sure that $\pi \equiv 1 \pmod 2$. This can be checked easily, the only non-obvious element in $2H$ being $2\varrho = 1 + i + j + k$. Thus $1 \equiv i + j + k$ and $1 + i \equiv j + k$ modulo 2. For example, $p = 17$ gives the positive solutions

$$(t, x, y, z) = (1, 4, 0, 0), (1, 0, 4, 0), (1, 0, 0, 4), (3, 2, 2, 0), (3, 2, 0, 2), (3, 0, 0, 2).$$

If t is assumed to be positive in all cases, 4 can be taken as ± 4 in the first three solutions, while the two 2's in the second triple can be replaced by ± 2. So there are $3 \cdot 2 + 3 \cdot 4 = 17 + 1$ monic primes over $p = 17$. For small primes, the positive solutions $\pi \equiv 1 \pmod 2$ of Eq. (26) are

p	positive solutions
3	0111
5	1200, 1020, 1002
7	2111
11	0113, 0131, 0311
13	3200, 3020, 3002, 1222
17	1400, 1040, 1004, 3220, 3202, 3002
19	4111, 0133, 0313, 0331
23	2331, 2313, 2133
29	5200, 5020, 5002, 3420, 3402, 3240, 3042, 3204, 3024
31	2511, 2151, 2115, 2333
37	1600, 1060, 1006, 5222, 1442, 1424, 1244

So $p = 37$ allows three solutions up to symmetry, 7 positive solutions, the first three with multiplicity 2, the others with multiplicity 8. For $p = 7$, the monic primes are

$$\begin{array}{llll} \pi_1 = 2 - i - j - k & \pi_2 = 2 - i + j + k & \pi_3 = 2 + i - j + k & \pi_4 = 2 + i + j - k \\ \pi_1^* = -2 - i - j - k & \pi_2^* = -2 - i + j + k & \pi_3^* = -2 + i - j + k & \pi_4^* = -2 + i + j - k \end{array}$$

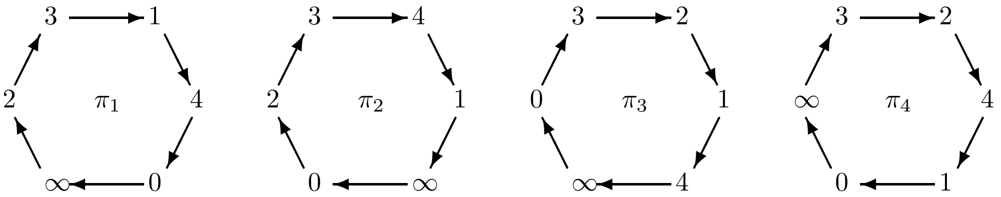
With $a = -5$ and $b = 3$, the corresponding matrices are

$$\begin{array}{llll} \pi_1 = \left(\begin{smallmatrix} 4 & -9 \\ -7 & 0 \end{smallmatrix}\right) & \pi_2 = \left(\begin{smallmatrix} 0 & 7 \\ 9 & 4 \end{smallmatrix}\right) & \pi_3 = \left(\begin{smallmatrix} 10 & 3 \\ 1 & -6 \end{smallmatrix}\right) & \pi_4 = \left(\begin{smallmatrix} -6 & -1 \\ -3 & 10 \end{smallmatrix}\right) \\ \pi_1^* = \left(\begin{smallmatrix} 0 & -9 \\ -7 & -4 \end{smallmatrix}\right) & \pi_2^* = \left(\begin{smallmatrix} -4 & 7 \\ 9 & 0 \end{smallmatrix}\right) & \pi_3^* = \left(\begin{smallmatrix} 6 & 3 \\ 1 & -10 \end{smallmatrix}\right) & \pi_4^* = \left(\begin{smallmatrix} -10 & -1 \\ -3 & 6 \end{smallmatrix}\right) \end{array} \tag{27}$$

For demonstration purposes, we have chosen a and b to satisfy Eq. (24) modulo $5 \cdot 7$, so that they can be used simultaneously for $p = 5$ and $p = 7$. If we abbreviate $(1 : c)$ with $c \in \mathbb{F}_7$ by c, and $(0 : 1)$ by ∞, the points in $\mathbb{P}^1(\mathbb{F}_7)$ associated with the matrices (27) are

0	1	2	3	4	5	6	∞
π_2^*	π_3	π_2	π_1	π_3^*	π_4^*	π_4	π_1^*

To let the primes over 7 act on the primes over 5, the matrices (27) can be reduced modulo 5, and the action coincides with the right action on $\mathbb{P}^1(\mathbb{F}_5)$. An easy calculation shows that the cycles of the action on $\mathbb{P}^1(\mathbb{F}_5)$ are as follows (the π_i^* give the inverse cycles):



Here the arrow $m \to n$ in the first hexagon means that $\pi_1 \to m = n$ in the L^*-algebra structure of $\mathbb{P}^1(\mathbb{F}_5)$.

In general, there may be fixed points. Forsyth et al. [16] have shown that except fixed points, all cycles in a metacommutation permutation have the same length. So it remains to determine the size of the circles to get the complete cycle structure. (In the preceding example, the cycles have maximal length, so that for each π_i there is just one cycle.)

Assume that p and q are distinct odd primes. For Hurwitz primes π, σ over p and q, respectively, we consider the L^*-algebra action $\sigma \mapsto (\pi \to \sigma)$. If t denotes the half-trace of π, the characteristic polynomial of $\varrho_q(\pi)$ is $\lambda^2 - 2t\lambda + p = 0$. So the eigenvalues are

$$\lambda = t \pm \sqrt{t^2 - p}.$$

With respect to the discriminant $d := t^2 - p$ there are three cases:

0.) $\varrho_q(\pi)$ elliptic (no fixed points): $\left(\frac{d}{q}\right) = -1$.

1.) $\varrho_q(\pi)$ parabolic (1 fixed point): $q | d$.

2.) $\varrho_q(\pi)$ hyperbolic (2 fixed points): $\left(\frac{d}{q}\right) = 1$.

The three cases are closely related to the structure of $\mathrm{PGL}_2(\mathbb{F}_q)$. Recall that the order of $\mathrm{PGL}_2(\mathbb{F}_q)$ is $(q+1)q(q-1)$. Let m be the size of the cycles in the permutation given by π acting on $\mathbb{P}^1(\mathbb{F}_q)$, and let n be the number of cycles.

Case 0: The eigenvalues of $\varrho_q(\pi)$ form a pair of conjugate elements $\lambda, \overline{\lambda} \in \mathbb{F}_{q^2}$. So the order of π in $\mathrm{PGL}_2(\mathbb{F}_q)$ coincides with the order of the matrix $\left(\begin{smallmatrix}\lambda & 0 \\ 0 & \overline{\lambda}\end{smallmatrix}\right)$. Now $\left(\begin{smallmatrix}\lambda & 0 \\ 0 & \overline{\lambda}\end{smallmatrix}\right)^n$ is a scalar matrix if and only if $\lambda^n = \overline{\lambda}^n$. So the size of the cycles is

$$m = \text{order of } \lambda \text{ in } \mathbb{F}_{q^2}^{\times}/\mathbb{F}_q^{\times},$$

and $mn = q + 1$. The sign of the permutation π is $\left(\frac{p}{q}\right) = (-1)^n$.

Case 1: The eigenvalue $\lambda = t$ of $\varrho_q(\pi)$ has multiplicity 2 and gives the single fixed point. Hence $mn = q$, and $m > 1$ implies that $m = q$. So there is one cycle of order q. The sign of the permutation π is $\left(\frac{p}{q}\right) = 1$.

Case 2: As there are two fixed points, $mn = q - 1$. There are two distinct eigenvalues $\lambda_1, \lambda_2 \in \mathbb{F}_q$. So the size of the cycles is given by

$$m = \text{order of } \tfrac{\lambda_1}{\lambda_2} \text{ in } \mathbb{F}_q^{\times}.$$

Here we also have $\left(\frac{p}{q}\right) = (-1)^n$.

Although this sign is the same for all π with $N(\pi) = p$, the cycle structure depends on the trace, as the following example shows.

Example 4. For $p = 13$, the half-trace t may be 1 or 3. Take $q = 37$. Then both cases are hyperbolic. For $t = 1$, the eigenvalues are $\lambda = 1 \pm \sqrt{-12} = 1 \pm 5$ (modulo 37). So we have $\frac{\lambda_1}{\lambda_2} = -\frac{6}{4} = 17$ (modulo 37). The order of 17 modulo 37 is 36. So there are two fixed points and one cycle of order 36.

For $t = 3$, the eigenvalues are $\lambda = 3 \pm \sqrt{-4} = 3 \pm 12$. Thus $\frac{\lambda_1}{\lambda_2} = \frac{15}{-9} = 23$. Now the order of 23 modulo 37 is 12. So there are three cycles of order 12. The parity of n is the same in both cases, namely, $\left(\frac{13}{37}\right) = -1$.

References

[1] A. Bigard, K. Keimel, S. Wolfenstein, Groupes et anneaux réticulés, Lecture Notes in Mathematics, vol. 608, Springer-Verlag, Berlin–New York, 1977.

[2] G. Birkhoff, Lattice ordered groups, Ann. of Math. 43 (1942) 298–331.

[3] B. Bosbach, Rechtskomplementäre Halbgruppen, Math. Z. 124 (1972) 273–288.

[4] S. Boyer, D. Rolfsen, B. Wiest, Orderable 3-manifold groups, Ann. Inst. Fourier (Grenoble) 55 (1) (2005) 243–288.

[5] E. Brieskorn, K. Saito, Artin-Gruppen und Coxeter-Gruppen, Invent. Math. 17 (1972) 245–271.

[6] F. Chouraqui, E. Godelle, Finite quotients of groups of I-type, Adv. Math. 258 (2014) 46–68.

[7] H. Cohn, A. Kumar, Metacommutation of Hurwitz primes, Proc. Amer. Math. Soc. 143 (4) (2015) 1459–1469.

[8] J.H. Conway, D.A. Smith, On Quaternions and Octonions: Their Geometry, Arithmetic, and Symmetry, A K Peters, Ltd., Natick, MA, 2003.

[9] P. Conrad, Right-ordered groups, Michigan Math. J. 6 (1959) 267–275.

[10] M.R. Darnel, Theory of Lattice-Ordered Groups, Monographs and Textbooks in Pure and Applied Mathematics, vol. 187, Marcel Dekker, Inc., New York, 1995.

[11] P. Dehornoy, Groupes de Garside, Ann. Sci. Éc. Norm. Supér. (4) 35 (2) (2002) 267–306.

[12] P. Dehornoy, F. Digne, E. Godelle, D. Krammer, J. Michel, Foundations of Garside Theory, EMS Tracts in Math., vol. 22, European Mathematical Society, 2015.

[13] P. Dehornoy, L. Paris, Gaussian groups and Garside groups, two generalisations of Artin groups, Proc. Lond. Math. Soc. (3) 79 (3) (1999) 569–604.

[14] P. Deligne, Les immeubles des groupes de tresses généralisés, Invent. Math. 17 (1972) 273–302.

[15] P. Etingof, T. Schedler, A. Soloviev, Set-theoretical solutions to the quantum Yang–Baxter equation, Duke Math. J. 100 (1999) 169–209.

[16] A. Forsyth, J. Gurev, S. Shrima, Metacommutation as a group action on the projective line over $\mathbb{F}_p$, Proc. Amer. Math. Soc. 144 (11) (2016) 4583–4590.

[17] D.J. Foulis, Conditions for the modularity of an orthomodular lattice, Pacific J. Math. 11 (1961) 889–895.

[18] L. Herman, E.L. Marsden, R. Piziak, Implication connectives in orthomodular lattices, Notre Dame J. Form. Log. 16 (1975) 305–328.

[19] A. Hurwitz, Über die Zahlentheorie der Quaternionen, Nachr. Ges. Wiss. Goett., Math.-Phys. Kl. (1896) 313–340.

[20] G. Kalmbach, Orthomodular Lattices, London Mathematical Society Monographs, vol. 18, Academic Press, Inc., London, 1983.

[21] L.H. Loomis, The lattice theoretic background of the dimension theory of operator algebras, Mem. Amer. Math. Soc. 18 (1955).

[22] J.-H. Lu, M. Yan, Y.-C. Zhu, On the set-theoretical Yang–Baxter equation, Duke Math. J. 104 (1) (2000) 1–18.

[23] W.A.J. Luxemburg, A.C. Zaanen, Riesz Spaces, Vol. I, North-Holland Mathematical Library, North-Holland Publishing Co. / American Elsevier Publishing Co., Amsterdam–London / New York, 1971.

[24] W.A.J. Luxemburg, A.C. Zaanen, Riesz Spaces, II, North-Holland Mathematical Library, vol. 30, North-Holland Publishing Co., Amsterdam, 1983.

[25] A. Navas, On the dynamics of (left) orderable groups, Ann. Inst. Fourier (Grenoble) 60 (5) (2010) 1685–1740.

[26] A. Navas, B. Wiest, Nielsen–Thurston orders and the space of braid orderings, Bull. Lond. Math. Soc. 43 (5) (2011) 901–911.

[27] I. Reiner, Maximal Orders, Corrected reprint of the 1975 original, With a foreword by M. J. Taylor, London Mathematical Society Monographs, New Series, vol. 28, The Clarendon Press, Oxford University Press, Oxford, 2003.

[28] W. Rump, A decomposition theorem for square-free unitary solutions of the quantum Yang–Baxter equation, Adv. Math. 193 (2005) 40–55.

[29] W. Rump, L-algebras, self-similarity, and l-groups, J. Algebra 320 (6) (2008) 2328–2348.

[30] W. Rump, Semidirect products in algebraic logic and solutions of the quantum Yang–Baxter equation, J. Algebra Appl. 7 (4) (2008) 471–490.

[31] W. Rump, Braces, radical rings, and the quantum Yang–Baxter equation, J. Algebra 307 (2007) 153–170.

[32] W. Rump, Right l-groups, geometric Garside groups, and solutions of the quantum Yang–Baxter equation, J. Algebra 439 (2015) 470–510.

[33] W. Rump, Decomposition of Garside groups and self-similar L-algebras, J. Algebra 485 (2017) 118–141.

[34] W. Rump, Von Neumann algebras, L-algebras, Baer *-monoids, and Garside groups, Forum Math., to appear.

[35] H. Short, B. Wiest, Orderings of mapping class groups after Thurston, Enseign. Math. 46 (3–4) (2000) 279–312.

[36] T. Traczyk, On the structure of BCK-algebras with $zx \cdot yx = zy \cdot xy$, Math. Jpn. 33 (2) (1988) 319–324.