DISTRIBUTIVE LATTICES, ASSOCIATIVE GEOMETRIES: THE ARITHMETIC CASE

WOLFGANG BERTRAM

Abstract. We prove an identity for five arguments, valid in the lattice of natural numbers with gcd and lcm as lattice operations. More generally, this identity characterizes arbitrary distributive lattices. Fixing three of the five arguments, we always get *associative* products, and thus every distributive lattice carries many semigroup structures. In the arithmetic case, we explicitly compute multiplication tables of such semigroups and describe some of their properties. Many of them are periodic, and can be seen as "non-commutative analogs" of the rings $\mathbb{Z}/n\mathbb{Z}$.

1. Introduction

For a quintuplet (x,a,y,b,z) of elements of a lattice $\mathcal{X}$ with operations $\wedge$ (meet) and $\vee$ (join), we define two other elements by

$$L = L(x,a,y,b,z) \ := \ \big(b\wedge(z\vee(a\wedge y))\big) \ \vee \ \big(z\wedge(b\vee(x\wedge y))\big) \ \vee \ \big(x\wedge(a\vee(z\wedge y))\big) \ \vee \ \big(a\wedge(x\vee(b\wedge y))\big), \tag{1.1}$$

$$U = U(x,a,y,b,z) \ := \ \big(a\vee(z\wedge(b\vee y))\big) \ \wedge \ \big(x\vee(b\wedge(z\vee y))\big) \ \wedge \ \big(z\vee(a\wedge(x\vee y))\big) \ \wedge \ \big(b\vee(x\wedge(a\vee y))\big). \tag{1.2}$$

The terms defining L and U will also be denoted by $L = L_1 \vee L_2 \vee L_3 \vee L_4$ and $U = U_1 \wedge U_2 \wedge U_3 \wedge U_4$ (related to two other terms L_5, U_5, cf. Eqn. (2.1)). We study the maps $L, U : \mathcal{X}^5 \to \mathcal{X}$ thus defined for the following kinds of lattices:

1. the *arithmetic case*: $\mathcal{X} = \mathbb{N}_0$ is the lattice of natural numbers (with 0), with $\wedge =$ lcm (*least common multiple*) and $\vee =$ gcd (*greatest common divisor*),
2. the *totally orderd*, or *chain case*: here M is a totally ordered set, with $\vee = \max$ and $\wedge = \min$,
3. the *power set case*: $\mathcal{X} = \mathcal{P}(M)$ is the power set of a set M, with $\wedge = \cap$ being intersection and $\vee = \cup$ union,
4. the *Grassmannian case*: W is a (right) module over a unital ring $\mathbb{K}$, and $\mathcal{X}$ the space of all submodules of W, with meet $\wedge = \cap$ and join $\vee = +$.

Theorem 1.1. *In cases* (1) – (3)*, we have* $U = L$*, i.e.,*

$$\forall x,a,y,b,z \in \mathcal{X} : \qquad L(x,a,y,b,z) = U(x,a,y,b,z). \tag{1.3}$$

In the Grassmannian case (4), we have $L \leq U$, i.e.,

$$\forall x,a,y,b,z \in \mathcal{X} : \qquad L(x,a,y,b,z) \subset U(x,a,y,b,z). \tag{1.4}$$

2010 *Mathematics Subject Classification.* 06D05 , 06D50 , 11A05 .

Key words and phrases. associative geometry, distributive lattice, gcd, lcm, semigroup .

The starting point of the present work was the discovery, triggered by computer checks (cf. Remark 6.3), that (to our big surprise), in the arithmetic case Inequality (1.4) becomes an equality. From the point of view of abstract lattice theory, this fact is explained as follows (Theorem 3.1):

Theorem 1.2. *Let $\mathcal{X}$ be a lattice. Then the following are equivalent:*

(i) *The identity $U = L$ holds in $\mathcal{X}$.*

(ii) *The lattice $\mathcal{X}$ is* distributive *: $\forall x, y, z \in \mathcal{X}$, $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$.*

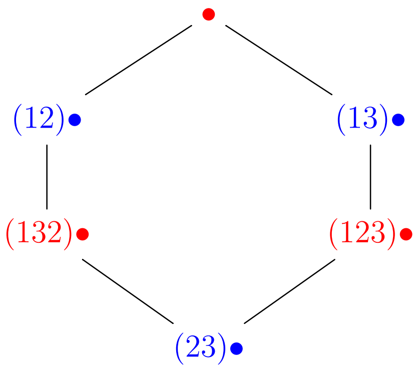
Moreover, we see that the lattice is *modular* when Inequality (1.4) holds, and one may conjecture that the converse also holds (see Remark 3.3) – we shall come back to this problem in subequent work.

The most important issue about the quintary map $L = U$ thus defined is that *fixing three of the five arguments, it defines associative products on $\mathcal{X}$.* More precisely, the "central" variable y shall be among the three fixed argments. For instance, fixing (a, y, b), we define the *principal product* $\bullet : \mathcal{X}^2 \to \mathcal{X}$ by

$$x \bullet z := x \bullet_{a,y,b} z := L(x, a, y, b, z) = U(x, a, y, b, z). \tag{1.5}$$

Because of the obvious invariance of L under the Klein four-group V acting on the variables $(x, a, b, z) = (v_1, v_2, v_3, v_4)$ (Lemma 2.1), we get $\frac{24}{4} = 6$ different kinds of "products" on $\mathcal{X}$. Following a terminology used by Conway and Smith ([CS03]), we present these six products as a "hexad" of products, labelled by the action of the symmetric group $\mathfrak{S}_3 = \mathfrak{S}_4 / V$ (e.g., $((23)\bullet)(x, z) = z \bullet x$ is the opposite product of $\bullet$; in general, opposite vertices correspond to opposite products),

(1.6)



Theorem 1.3. *Let $\mathcal{X}$ be a distributive lattice. Then the six products given by the above "hexad" are all* associative. *In other terms, they define semigroup structures on $\mathcal{X}$. These semigroups are* weak bands, *in the sense that they satisfy the identity*

$$\forall v, w \in \mathcal{X} : \qquad v^2 w = vw = vw^2.$$

Instead of checking associativity by direct (and necessarily long) computation, we proceed by using *representation theory for distributive lattices*: they can be imbedded into power set lattices (case (3) mentioned above); and in the power set case, we can decompose the product into "atoms", where the atoms are six elementary products called "true, false, left, right, and, or", and which obviously are associative and weak bands.

In the arithmetic case, we study these products further: many of them are *periodic*, and then essentially reduce to *finite semigroups* (Theorem 6.4). In Section 6, we give several examples of "multiplication tables" of such finite semigroups. To give an idea, the product $x \bullet_{3,2,4} z$ has "column period" 3, and "line period" 4:

$x \bullet_{3,2,4} z$	0	1	2	3	4	5	6
0	12	4	4	12	4	4	12
1	3	1	1	3	1	1	3
2	6	2	2	6	2	2	6
3	3	1	1	3	1	1	3
4	12	4	4	12	4	4	12

To illustrate associativity: $(5 \bullet 6) \bullet 6 = 3 \bullet 6 = 3 = 5 \bullet 6 = 5 \bullet (6 \bullet 6)$. Note that the set $\{1, \ldots, 12\}$, as well as the set of divisors of 12, form semigroups for $\bullet$. Principal products are periodic, and thus can be seen as analogs of the usual quotient rings $\mathbb{Z}/n\mathbb{Z}$. The parastrophes are not always periodic. One may wonder if these semigroups have non-trivial applications in number theory.

Motivation for the present work comes from joint work with Michael Kinyon on *associative geometries*, [BeKi10a, BeKi10b, BeKi12]. An associative geometry has as underlying space a *Grassmannian* (case (4) in the above list), whence an underlying lattice structure playing an important role in the theory. The algebraic structure of an associative geometry is encoded by a quintary *structure map* $\Gamma : \mathcal{X}^5 \to \mathcal{X}$, $(x, a, y, b, z) \mapsto \Gamma(x, a, y, b, z)$. This structure map has interesting algebraic properties showing a "geometric flavor". Thus it is a natural question to ask how it looks like in the *arithmetic case* $W = \mathbb{K} = \mathbb{Z}$, and to find a good algorithm for computing it. The answer is that, in this case, simply $L = \Gamma = U$, which furnishes an excellent algorithm. In the case of general Grassmannians, the situation is much more complicated – we intend to study the relation between L, U and Γ in the case of Grassmannians, and of modular lattices, in subsequent work.

Acknowledgment. I thank Michael Kinyon for helpful comments, and for having first checked the equivalence (i) ⇔ (ii) from Theorem 1.2 by using the automated theorem prover Prover9.

2. Prelimary remarks on the general case

In every lattice $\mathcal{X}$, the expressions $L, U, L_1, \ldots, U_4$ defined by (1.1), (1.2), are closely related to the following expressions (see the following proof for explanations concerning the labelling)

$$L_5 := L_5^{(3)} := (b \wedge z) \vee (a \wedge x), \qquad U_5 := U_5^{(2)} := (a \vee z) \wedge (b \vee x), \tag{2.1}$$

$$L_5^{(1)} := (b \wedge a) \vee (z \wedge x), \qquad U_5^{(1)} := (a \vee b) \wedge (z \vee x), \tag{2.2}$$

$$L_5^{(2)} := (b \wedge x) \vee (a \wedge z), \qquad U_5^{(3)} := (a \vee x) \wedge (b \vee z). \tag{2.3}$$

Lemma 2.1. *In any lattice, the expressions $L(x, a, y, b, z)$ and $U(x, a, y, b, z)$ defined by (1.1) and (1.2) are invariant under the action of the Klein 4-group (double transpositions), acting on the variables (x, a, b, z), and so are the terms $L_5, \ldots, U_5^{(3)}$ defined above.*

Proof. This follows immediately from the definitions. For instance, exchanging simultaneously (a,b) and (x,z) exchanges (L_2,L_3) and (L_1,L_4), and so on; due to commutativity of $\wedge$ and $\vee$, the order is irrelevant. More formally, to fix the action of the symmetric group $\mathfrak{S}_5$ on the five variables, we fix the correspondence

$$\mathbf{x} := (x_1,x_2,x_5,x_3,x_4) := (x,a,y,b,z).$$

We let act $\mathfrak{S}_4$ on the variables $(x,a,b,z) = (x_1,x_2,x_3,x_4)$, and $\mathfrak{S}_3$ on $(x,a,b) = (x_1,x_2,x_3)$, in the usual way, and hence these groups also act on functions of these variables, like $L_1,\ldots,U_5$. Thus, for instance, $L_5^{(3)}$ is obtained by applying the transposition (13) to $L_5^{(1)}$, and so on. Note that the upper index 3 in $L_5^{(3)}$ indicates the variable $x_3 = b$ with which $x_4 = z$ is paired via $b \wedge z$ in Formula (2.1), etc. □

As we will see, in general lattices, $L(x,a,y,b,z)$ is in general different from $U(x,a,y,b,z)$. However, some "diagonal values" of L and U always agree:

Theorem 2.2. *Let $(\mathcal{X},\wedge,\vee)$ be a lattice and $(x,a,y,b,z) \in \mathcal{X}^5$. Then:*

(1) for $a = z$ and $b = x$, we get $L(x,z,y,x,z) = z \wedge x = U(x,z,y,x,z)$,
(2) for $b = z$ and $x = a$, we get $L(x,x,y,z,z) = x \vee z = U(x,x,y,z,z)$,
(3) for $a = y = b$, we get $L(x,y,y,y,z) = y = U(x,y,y,y,z)$,
(4) if $\mathcal{X}$ is bounded, with maximal element 1 and minimal element 0, then

$$\begin{aligned}
&L(x,1,0,1,z) = x \vee z = U(x,1,0,1,z),\\
&L(x,0,1,0,z) = x \wedge z = U(x,0,1,0,z),\\
&L(x,1,1,0,z) = x = U(x,1,1,0,z),\\
&L(x,0,0,1,z) = z = U(x,0,0,1,z),\\
&L(x,a,0,b,z) = L_5(x,a,y,b,z) = (b \wedge z) \vee (a \wedge x),\\
&U(x,a,1,b,z) = U_5(x,a,y,b,z) = (a \vee z) \wedge (b \vee x),\\
&L(x,0,y,b,z) = L_2(x,a,y,b,z) = z \wedge (b \vee (x \wedge y)),\\
&U(x,1,y,b,z) = U_2(x,a,y,b,z) = x \vee (b \wedge (z \wedge y)).
\end{aligned}$$

Proof. All claims follow by direct computation using the defining identities of a lattice, in particular, $a \vee (a \wedge x) = a = a \wedge (a \vee x)$. □

Lemma 2.3. *The function L is* monotonic*: if $\mathbf{x} \leq \mathbf{x}'$ (meaning that $x_i \leq x_i'$ for $i = 1,\ldots,5$), then $L(\mathbf{x}) \leq L(\mathbf{x}')$. The same holds for U, L_i, U_i, $i = 1,\ldots,5$. Moreover, for $i = 1,\ldots,4$,*

$$L_i \leq L, \qquad U \leq U_i,$$

and when the lattice $\mathcal{X}$ is bounded, this also holds for $i = 5$.

Proof. Since both $\wedge$ and $\vee$ are monotonic operations, the same holds for L, etc. The inequalities for $i = 1,\ldots,4$ follow directly from the definition of L, resp. U, as join, resp. meet, of these expressions. For $i = 5$, in the bounded case, this follows by monotony from Item (4) of the preceding theorem, since $0 \leq y$ and $y \leq 1$. □

Clearly, monotonic lattice morphisms induce morphisms of L and of U. The following is obvious from Formulae (1.1), (1.2):

Lemma 2.4. *If $\phi : \mathcal{X} \to \mathcal{X}$ is an* antitone lattice morphism*, i.e., $\phi(a \vee b) = \phi(a) \wedge \phi(b)$ and $\phi(a \wedge b) = \phi(a) \vee \phi(b)$, then*

$$\begin{aligned} \phi L(x,a,y,b,z) &= U(\phi x, \phi b, \phi y, \phi a, \phi z), \\ \phi U(x,a,y,b,z) &= L(\phi x, \phi b, \phi y, \phi a, \phi z). \end{aligned}$$

3. Characterization of distributive lattices

Recall that a lattice $\mathcal{X}$ is called *distributive* if, for all $x, y, z \in \mathcal{X}$,

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z).$$

This is equivalent to the dual identity

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z).$$

Theorem 3.1. *For every lattice $\mathcal{X}$, the following properties are equivalent:*

(i) *The identity $U = L$ holds in $\mathcal{X}$.*
(ii) *The lattice $\mathcal{X}$ is distributive.*

Proof. (ii) ⇒ (i): If $\mathcal{X}$ is distributive, the expressions L_i, U_i can be transformed

$$\begin{aligned} L_1 &= (b \wedge (z \vee (a \wedge y))) = (b \wedge z) \vee (b \wedge a \wedge y), \\ L_2 &= (z \wedge b) \vee (z \wedge x \wedge y), \\ L_3 &= (x \wedge a) \vee (x \wedge z \wedge y), \\ L_4 &= (a \wedge x) \vee (a \wedge b \wedge y), \\ U_1 &= (a \vee (z \wedge (b \vee y))) = (a \vee z) \wedge (a \vee b \vee y) \\ U_2 &= (x \vee b) \wedge (x \vee z \vee y) \\ U_3 &= (z \vee a) \wedge (z \vee x \vee y) \\ U_4 &= (b \vee x) \wedge (b \vee a \vee y). \end{aligned}$$

Using this, we get, using the terms defined by (2.1), (2.2), (2.3),

$$L = (a \wedge x) \vee (b \wedge z) \vee (a \wedge b \wedge y) \vee (x \wedge z \wedge y) = L_5^{(3)} \vee (L_5^{(1)} \wedge y), \tag{3.1}$$

$$U = (a \vee z) \wedge (x \vee b) \wedge (a \vee b \vee y) \wedge (x \vee z \vee y) = U_5^{(2)} \wedge (U_5^{(1)} \vee y), \tag{3.2}$$

where we have abbreviated $L_5^{(i)} = L_5^{(i)}(x,a,y,b,z)$, and $U_5^{(i)} = U_5^{(i)}(x,a,y,b,z)$. These elements generate a lattice having a remarkably simple structure:

Proposition 3.2. *Fix elements x, a, b, z in a distributive lattice $\mathcal{X}$. Then for $\{i,j,k\} = \{1,2,3\}$, writing $L_5^{(i)} = L_5^{(i)}(x,a,y,b,z)$, and $U_5^{(i)} = U_5^{(i)}(x,a,y,b,z)$,*

$$U_5^{(i)} \wedge U_5^{(j)} = L_5^{(k)}, \qquad L_5^{(i)} \vee L_5^{(j)} = U_5^{(k)}.$$

The 6 *elements* $L_5^{(i)}, U_5^{(i)}$ *(*$i=1,2,3$*) generate a lattice of* 8 *elements, which is a homomorphic image of the lattice of subsets of* $\{1,2,3\}$*, as indicated by the diagram:*

$$\begin{tikzcd}
& U_5^{(3)} \vee U_5^{(2)} \vee U_5^{(1)} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
U_5^{(3)} \arrow[d, dash] \arrow[dr, dash] & U_5^{(2)} \arrow[dl, dash] \arrow[dr, dash] & U_5^{(1)} \arrow[dl, dash] \arrow[d, dash] \\
L_5^{(1)} \arrow[dr, dash] & L_5^{(2)} \arrow[d, dash] & L_5^{(3)} \arrow[dl, dash] \\
& L_5^{(1)} \wedge L_5^{(2)} \wedge L_5^{(3)} &
\end{tikzcd}$$

Proof. In the following, we drop the lower index 5. For instance, if $(i,j,k)=(1,2,3)$, then by distributivity,

$$L^{(3)} = (b \wedge z) \vee (a \wedge x) = (b \vee a) \wedge (z \vee x) \wedge (b \vee x) \wedge (z \vee a) = U^{(1)} \wedge U^{(2)},$$

and similarly for the other relations. It follows, for $\{1,2,3\}=\{i,j,k\}$, that

$$\begin{aligned} L^{(i)} \wedge L^{(j)} &= (U^{(j)} \wedge U^{(k)}) \wedge (U^{(i)} \wedge U^{(k)}) \\ &= U^{(1)} \wedge U^{(2)} \wedge U^{(3)} \\ &= L^{(i)} \wedge L^{(k)}, \end{aligned}$$

whence

$$L^{(i)} \wedge L^{(j)} = L^{(1)} \wedge L^{(2)} \wedge L^{(3)}.$$

In the same way,

$$U^{(i)} \vee U^{(j)} = L^{(1)} \vee L^{(2)} \vee L^{(3)} = U^{(1)} \vee U^{(2)} \vee U^{(3)}$$

which implies also $U^{(i)} \wedge L^{(i)} = L^{(1)} \vee L^{(2)} \vee L^{(3)}$, etc. □

As a particular case of the proposition, we have

$$U_5^{(2)} \wedge L_5^{(3)} = (L_5^{(1)} \vee L_5^{(3)}) \wedge L_5^{(3)} = L_5^{(3)} = U_5^{(1)} \wedge U_5^{(2)}.$$

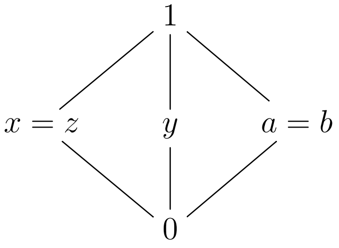
This is used in the fifth equality of the followig computation, along with distributivity and the relation $L_5^{(3)} \vee L_5^{(1)} = U_5^{(2)}$:

$$\begin{aligned} L &= L_5^{(3)} \vee (L_5^{(1)} \wedge y) \\ &= (L_5^{(3)} \vee L_5^{(1)}) \wedge (L_5^{(3)} \vee y) \\ &= U_5^{(2)} \wedge (L_5^{(3)} \vee y) \\ &= (U_5^{(2)} \wedge L_5^{(3)}) \vee (U_5^{(2)} \wedge y) \\ &= (U_5^{(1)} \wedge U_5^{(2)}) \vee (U_5^{(2)} \wedge y) \\ &= U_5^{(2)} \wedge (U_5^{(1)} \vee y) = U, \end{aligned}$$

(i) $\Rightarrow$ (ii): Since every non-distributive lattice contains a sublattice isomorphic to the diamond lattice M_3 or to the pentagon lattice N_5 (see [BS]), it is enough to show that the identity $L = U$ is not satisfied in M_3 and in N_5. First assume that $\mathcal{X}$ is the *diamond lattice*

$$M_3 = \{0, u, v, w, 1\}, \quad u \wedge v = 0 = u \wedge w = v \wedge w, \quad u \vee v = 1 = v \vee w = w \vee u,$$

and choose $x = z = u$, $y = v$, $a = b = w$, as indicated by the Hasse diagram:

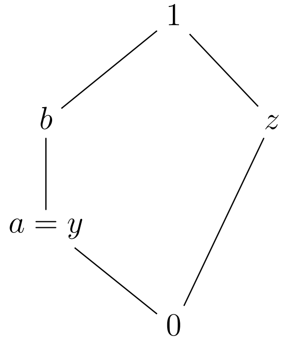


We have $a \wedge y = 0 = x \wedge y = z \wedge y = b \wedge y$, and $a \vee y = 1 = x \vee y = z \vee y = b \vee y$, and (with the four terms ordered as in Equations (1.1) and (1.2)

$$\begin{aligned} L(x, a, y, a, x) &= (b \wedge z) \vee (z \wedge b) \vee (x \wedge a) \vee (b \wedge x) \\ &= 0 \vee 0 \vee 0 \vee 0 = 0, \\ U(x, a, y, a, x) &= (a \vee z) \wedge (x \vee b) \wedge (x \vee a) \wedge (b \vee x) \\ &= 1 \wedge 1 \wedge 1 \wedge 1 = 1. \end{aligned}$$

Thus $L = U$ does not hold in M_3. Next, assume that $\mathcal{X} = N_5$ is the *pentagon lattice*, and choose $a = y = u$, $b = w$, $z = v$, and x any of the elements of N_5:

$$N_5 = \{0, u, v, w, 1\}, \qquad 0 < u < w < 1, \quad 0 < v < 1,$$



Since $L = L_1 \vee L_2 \vee L_3 \vee L_4$, we have $L_1 \leq L$, and likewise $U \leq U_1$. But

$$\begin{aligned} L_1 &= b \wedge (z \vee (a \wedge y)) = b \wedge (z \vee a) = b \wedge 1 = b, \\ U_1 &= a \vee (z \wedge (b \vee y)) = a \vee (z \wedge b) = a \vee 0 = a, \end{aligned}$$

whence $U \leq U_1 = a < b = L_1 \leq L$, and hence L is not equal to U in N_5. □

Remark 3.1. The characterization of distributive lattices by the identity $L = U$ can be seen as a "higher" analog of the known fact (cf. [Bi], II., Theorem 8) that $\mathcal{X}$ *is distributive iff it satisfies the median law*

$$(x \vee y) \wedge (y \vee z) \wedge (z \wedge x) = (x \wedge y) \vee (y \wedge z) \vee (y \wedge x).$$

Remark 3.2. The cubic lattice from Prop. 3.2 can be seen as part of the free distributive lattice on 4 generators. Its top element is the join of the 6 possible meets of the generators, and its bottom element the meet of the 6 possible joins. When two of the generators coincide (say, $x = a$), then we get another part, which is just a square (say, $L^{(1)} = U^{(2)} = L^{(3)}$ and $U^{(1)} = L^{(2)} = U^{(3)}$). This square is the product of the trivial lattice given by the median element (preceding remark) and a lattice with 2 generators.

Corollary 3.3. *The following identities hold:*

1. *In the* arithmetic case *(lattice $\mathbb{N}_0$ with $\vee = \mathrm{gcd}$, $\wedge = \mathrm{lcm}$)*
$$\mathrm{gcd}\big(\mathrm{lcm}(a,x), \mathrm{lcm}(b,z), \mathrm{lcm}(a,b,y), \mathrm{lcm}(x,y,z)\big) = \\ \mathrm{lcm}(\mathrm{gcd}(a,z), \mathrm{gcd}(x,b), \mathrm{gcd}(a,b,y), \mathrm{gcd}(x,y,z)).$$
2. *In the* totally ordered case *(chain with $\vee = \max$, $\wedge = \min$)*
$$\max(\min(a,x), \min(b,z), \min(a,b,y), \min(x,y,z)) = \\ \min(\max(a,z), \max(x,b), \max(a,b,y), \max(x,y,z)).$$
3. *In the* Boolean case *(power set $\mathcal{X} = \mathcal{P}(M)$ with $\vee = \cup$, $\wedge = \cap$)*
$$(a \cap x) \cup (b \cap z) \cup (a \cap b \cap y) \cup (x \cap y \cap z) = \\ (a \cup z) \cap (x \cup b) \cap (a \cup b \cup y) \cap (x \cup y \cup z).$$

Proof. All three lattices are well-known to be distributive, hence satisfy $L = U$ in the form given by (3.1) and (3.2). □

Theorem 3.4. *Assume $\mathcal{X}$ is a lattice satisfying the identity $L \leq U$. Then this lattice is modular.*

Proof. If $\mathcal{X}$ is not modular, then it contains the pentagon lattice N_5 as sublattice (see [Bi], I., Theorem 12), and as we have seen in the preceding proof, $L \leq U$ does not hold in N_5. □

Remark 3.3. What about the converse: does modularity imply $L \leq U$? As mentioned in the introduction, the identity $L \leq U$ does hold in Grassmannians, which form an important class of modular lattices. We shall come back to this question in subsequent work.

Theorem 3.5. *Let $\mathcal{X}$ be a distributive lattice, and $\phi : \mathcal{X} \to \mathcal{X}$ antitone. Then*
$$\phi U(x,a,y,b,z) = U(\phi x, \phi b, \phi y, \phi a, \phi z).$$
In particular, this holds when $\mathcal{X}$ is a Boolean algebra (complemented distributive lattice), with complement map $\phi = \neg : \mathcal{X} \to \mathcal{X}$.

Proof. This follows from $U = L$, together with Lemma 2.4. □

Example 3.1. The lattice $\mathbb{N}_0$ does not carry any anti-automorphism. But let $N \in \mathbb{N}$, $N > 1$, and K a divisor of N. Then the distributive lattice (interval) $\mathcal{X} = [K,N] = \{d \in \mathbb{N} \mid K|d,\ d|N\}$ carries an anti-automorphism $\phi(d) = \frac{KN}{d}$. If $\frac{N}{K}$ contains only simple prime-powers as factors, then ϕ is a complement map, but otherwise it's not.

In the distributive case, the six versions $\sigma.L = \sigma.U$ ($\sigma \in \mathfrak{S}_3$) of $L = U$, organized as a "hexad" according to the scheme from (1.6), are explicitly given as follows, in terms of $L_5^{(i)}$ and $U_5^{(i)}$. We use that $\sigma.L_5^{(i)} = L_5^{(\sigma(i))}$, resp. $\sigma.U_5^{(i)} = U_5^{(\sigma(i))}$. Note that the invariance group in $\mathfrak{S}_4$ of each term $L_5^{(i)}$, resp., $U_5^{(i)}$, is the subgroup of order 8 generated by the Klein 4-group together with the transposition $(i4)$. There are 3 such subgroups, all isomorphic to a dihedral group D_4.

$$\begin{tikzcd}
 & L = L_5^{(3)} \vee (L_5^{(1)} \wedge y) \arrow[dl, dash] \arrow[dr, dash] & \\
(12)L = L_5^{(3)} \vee (L_5^{(2)} \wedge y) \arrow[d, dash] & & (13)L = L_5^{(1)} \vee (L_5^{(3)} \wedge y) \arrow[d, dash] \\
(132)L = L_5^{(2)} \vee (L_5^{(3)} \wedge y) \arrow[dr, dash] & & (123)L = L_5^{(1)} \vee (L_5^{(2)} \wedge y) \arrow[dl, dash] \\
 & (23)L = L_5^{(2)} \vee (L_5^{(1)} \wedge y) &
\end{tikzcd}$$

When $L = U$, this hexad coincides with

$$\begin{tikzcd}
 & U = U_5^{(2)} \wedge (U_5^{(1)} \vee y) \arrow[dl, dash] \arrow[dr, dash] & \\
(12)U = U_5^{(1)} \wedge (U_5^{(2)} \vee y) \arrow[d, dash] & & (13)U = U_5^{(2)} \wedge (U_5^{(3)} \vee y) \arrow[d, dash] \\
(132)U = U_5^{(1)} \wedge (U_5^{(3)} \vee y) \arrow[dr, dash] & & (123)U = U_5^{(3)} \wedge (U_5^{(2)} \vee y) \arrow[dl, dash] \\
 & (23)U = U_5^{(3)} \wedge (U_5^{(1)} \vee y) &
\end{tikzcd}$$

Remark 3.4. Under *duality of lattices*, i.e., exchange of $\wedge$ and $\vee$, that is, exchange of $\leq$ and $\geq$, $U_5^{(i)}$ and $L_5^{(i)}$ exchange, for $i = 1, 2, 3$, and hence the first hexad exchanges with the "dual" of the second (where by "dual" hexad we mean the one obtained after applying a central symmetry). When the lattice is distributive, duality thus correponds to central symmetry.

4. A glimpse on the chain case

The statement of Item (2) of Corollary 3.3 can be refined:

Theorem 4.1. *Let M be a totally ordered set, with $\wedge = \min$ and $\vee = \max$. Then*

(1) if $a \leq y \leq b$, then $U = L = \max(a, \min(z, b)) = \min(\max(a, z), b)$,
(2) if $b \leq y \leq a$, then $U = L = \min(a, \max(x, b)) = \max(\min(a, x), b)$,
(3) if $x \leq y \leq z$, then $U = L = \max(x, \min(b, z)) = \min(\max(x, b), z)$,
(4) if $z \leq y \leq x$, then $U = L = \min(x, \max(a, z)) = \max(\min(x, a), z)$,

(5) if $a, b \leq y \leq x, z$, then $U = L = y$,
(6) if $x, z \leq y \leq a, b$, then $U = L = y$,
(7) if $a, x, b, z \leq y$, then $U = L = L_5 = \min(\max(b, z), \max(a, x))$,
(8) if $y \leq a, x, b, z$, then $U = L = U_5 = \max(\min(a, z), \min(b, x))$.

Proof. This follows in each case by inspection of the expressions appearing in Item (2) of Corollary 3.3. (In principle, there are $5! = 120$ cases to be checked; due to invariance under double transpositions, this reduces to 30 cases, which can be checked by hand or by machine.) □

Remark 4.1. What is the order-theoretic interpretation of these relations? Just as the total order $\leq$ is encoded by min and max, the expression $L = U$ should encode some order-theoretic concept. One may think of the *cyclic order* corresponding to the total order, defined on the one-point completion of M. When $M = \mathbb{R}$, then this one-point completion is the projective line $\mathbb{RP}^1 = S^1$, and L is in this case related to the *cross-ratio*. Thus L could play the role of a "cross-ratio type invariant for chains".

5. Associativity

In a distributive lattice $\mathcal{X}$, fixing a triple (a, y, b), we define a binary "product"

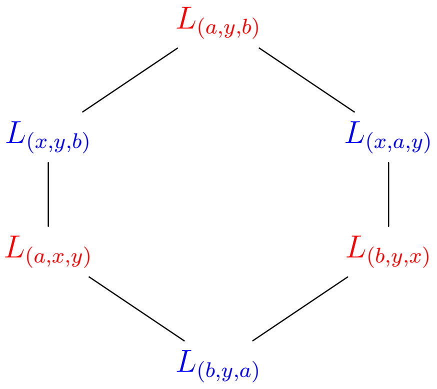
$$x \bullet z := x \cdot_{a,y,b} z := L(x, a, y, b, z) = U(x, a, y, b, z). \tag{5.1}$$

We are going to show that this product is always associative, hence defines a semigroup struture on $\mathcal{X}$. More generally, let us define:

Definition 5.1. *Let $\mathcal{X}$ be an arbitrary lattice. Fixing three of the five components of $\mathcal{X}^5$, we define "product maps" $\mathcal{X}^2 \to \mathcal{X}$ by considering the remaining two components as "variables". More specifically, the central component y shall always belong to the "fixed" variables. Explicitly, for $(x, a, y, b, z) \in \mathcal{X}^5$, we let*

$$\begin{aligned}
L^{(x,z)}_{(a,y,b)} &:= L^{(z,x)}_{(b,y,a)} := x \bullet^L_{a,y,b} z := L(x, a, y, b, z) = L(z, a, y, b, x) \\
L^{(a,z)}_{(x,y,b)} &:= L^{(z,a)}_{(b,y,x)} := L(x, a, y, b, z) = L(a, z, y, x, b), \\
L^{(b,z)}_{(x,a,y)} &:= L^{(z,b)}_{(a,x,y)} := L(x, a, y, b, z) = L(a, x, b, z, b).
\end{aligned}$$

Retaining only the subscripts, this is represented by the "hexad" of binary products



The same definitions and conventions can be given for U, and for any other quintary map $\mathcal{X}^5 \to \mathcal{X}$ that is invariant under the Klein 4-group acting on (x, a, b, z). In other words, the "hexad" (5.1) comes from $\bullet$ via the canonical action of the group $\mathfrak{S}_3 = \mathfrak{S}_4/V$ acting on the 4 variables $(v_1, v_2, v_3, v_4) = (x, a, b, z)$ (Diagram (1.6)). Following a terminology from the theory of loops and quasigroups, for a fixed triple (a, y, b), we call the six products in the "hexad" given above the parastrophes *of the "principal" product $\bullet$.*

Theorem 5.2. *Let $\mathcal{X}$ be a bounded distributive lattice, and fix a triple of elements in $\mathcal{X}$. Then any of the six products by the "hexad" given above is associative. Products belonging to opposite vertices of the hexad are opposite in the algebraic sense ($u \cdot^{\mathrm{op}} v = v \cdot u$). In particular, products of type $L_{a,y,a}$ or $L_{a,a,y}$ are commutative. Moreover, all semigroups $(\mathcal{X}, \cdot)$ thus obtained are* weak bands*, i.e., left and right multiplications are idempotent:*

$$\forall u, v \in \mathcal{X} : \qquad u(uv) = uv = (uv)v.$$

Proof. By the representation theorem for bounded distributive lattices ([S38], cf. [Bi], Chapter IX, Theorem 11), we can imbed $\mathcal{X}$ as a sublattice into the lattice of subsets $\mathcal{P}(M)$ of a set M. Associativity (and the weak band property) are algebraic identities for L in the sense of universal algebra; if they hold in the lattice $\mathcal{P}(M)$, then they hold also in the lattice $\mathcal{X}$. Thus we shall assume in the sequel that $\mathcal{X} = \mathcal{P}(M)$, and we prove the claim in this case. The advantage of $\mathcal{P}(M)$ is that it has a *complementation*, which makes it a *Boolean lattice*.

Definition 5.3. *Assume $\mathcal{X} = \mathcal{P}(M)$, and denote for $u \in \mathcal{X}$ by $\neg u := M \setminus u$ its complement. Fix a triple $(a, y, b) \in \mathcal{X}^3$. With respect to this datum, we decompose*

$$M = M^{\mathrm{true}} \sqcup M^{\mathrm{false}} \sqcup M^{\mathrm{right}} \sqcup M^{\mathrm{left}} \sqcup M^{\mathrm{and}} \sqcup M^{\mathrm{or}}$$

into a disjoint union of six subsets, as follows:

(1) $M^{\mathrm{true}} := a \wedge y \wedge b$
(2) $M^{\mathrm{false}} := \neg a \wedge \neg y \wedge \neg b$
(3) $M^{\mathrm{right}} := b \setminus a = b \wedge (\neg a)$
(4) $M^{\mathrm{left}} := a \setminus b = a \wedge (\neg b)$
(5) $M^{\mathrm{or}} := (a \wedge b) \setminus y = a \wedge b \wedge (\neg y)$
(6) $M^{\mathrm{and}} := y \setminus (a \vee b) = y \wedge (\neg a) \wedge (\neg b)$

In other words, an element $\omega \in M$ belongs to these sets iff the triple of propositions $(\omega \in a, \omega \in y, \omega \in b)$ has the following Boolean values:

(1) $(1, 1, 1)$
(2) $(0, 0, 0)$
(3) $(0, 0, 1)$ *or* $(0, 1, 1)$
(4) $(1, 0, 0)$ *or* $(1, 1, 0)$
(5) $(1, 0, 1)$
(6) $(0, 1, 0)$

Remark 5.1. The following arguments not only establish associativity of the "principal" product (5.1), but also give an independent proof of the identity $L = U$ in case of a power set lattice $\mathcal{X} = \mathcal{P}(M)$.

Now let $(x,a,y,b,z) \in \mathcal{X}^5$ and $\omega \in M$. Then ω may belong, or not, to some of the 5 compenents of this quintuplet – there are $2^5 = 32$ possible cases. In the following tables, we write 0 if ω does not belong to the set, and 1 if ω belongs to the set. These 32 cases can be partitioned according to the 6 cases defined above, as follows. For further information, we list also the Boolean values for ω belonging to elements of the lists $\mathtt{L} = (L_1, L_2, L_3, L_4)$ and $\mathtt{U} = (U_1, U_2, U_3, U_4)$, as well as for L_5 and U_5.

(1) Let $\omega \in M^{\mathrm{true}}$. The Boolean values for $\omega \in$ (or $\notin$) L, U, L_1, U_1, L_4, U_4 all coincide.

x	a	y	b	z	list $\mathtt{L}$	$\vee\mathtt{L} = \wedge\mathtt{U}$	list $\mathtt{U}$	L_5	U_5
1	1	1	1	1	$(1,1,1,1)$	1	$(1,1,1,1)$	1	1
1	1	1	1	0	$(1,0,1,1)$	1	$(1,1,1,1)$	1	1
0	1	1	1	1	$(1,1,0,1)$	1	$(1,1,1,1)$	1	1
0	1	1	1	0	$(1,0,0,1)$	1	$(1,1,1,1)$	0	1

(2) Let $\omega \in M^{\mathrm{false}}$. The Boolean values for $\omega \in$ (or $\notin$) L, U, L_1, U_1, L_4, U_4 coincide.

x	a	y	b	z	list $\mathtt{L}$	$\vee\mathtt{L} = \wedge\mathtt{U}$	list $\mathtt{U}$	L_5	U_5
0	0	0	0	0	$(0,0,0,0)$	0	$(0,0,0,0)$	0	0
0	0	0	0	1	$(0,0,0,0)$	0	$(0,0,1,0)$	0	0
1	0	0	0	0	$(0,0,0,0)$	0	$(0,1,0,0)$	0	0
1	0	0	0	1	$(0,0,0,0)$	0	$(0,1,1,0)$	0	1

(3) Let $\omega \in M^{\mathrm{right}}$. The Boolean values for $\omega \in$ (or $\notin$) L, U, L_1, U_1, L_5, U_5 coincide.

x	a	y	b	z	list $\mathtt{L}$	$\vee\mathtt{L} = \wedge\mathtt{U}$	list $\mathtt{U}$	L_5	U_5
0	0	0	1	0	$(0,0,0,0)$	0	$(0,0,0,1)$	0	0
0	0	0	1	1	$(1,1,0,0)$	1	$(1,1,1,1)$	1	1
1	0	0	1	0	$(0,0,0,0)$	0	$(0,1,0,1)$	0	0
1	0	0	1	1	$(1,1,0,0)$	1	$(1,1,1,1)$	1	1
0	0	1	1	0	$(0,0,0,0)$	0	$(0,1,0,1)$	0	0
0	0	1	1	1	$(1,1,0,0)$	1	$(1,1,1,1)$	1	1
1	0	1	1	0	$(0,0,0,0)$	0	$(0,1,0,1)$	0	0
1	0	1	1	1	$(1,1,0,0)$	1	$(1,1,1,1)$	1	1

(4) Let $\omega \in M^{\mathrm{left}}$. The Boolean values for $\omega \in$ (or $\notin$) L, U, L_4, U_4, L_5, U_5 coincide.

x	a	y	b	z	list $\mathtt{L}$	$\vee\mathtt{L} = \wedge\mathtt{U}$	list $\mathtt{U}$	L_5	U_5
0	1	0	0	0	$(0,0,0,0)$	0	$(1,0,0,0)$	0	0
0	1	0	0	1	$(0,0,0,0)$	0	$(1,0,1,0)$	0	0
1	1	0	0	0	$(0,0,1,1)$	1	$(1,1,1,1)$	1	1
1	1	0	0	1	$(0,0,1,1)$	1	$(1,1,1,1)$	1	1
0	1	1	0	0	$(0,0,0,0)$	0	$(1,0,0,0)$	0	0
0	1	1	0	1	$(0,0,0,0)$	0	$(1,0,1,0)$	0	0
1	1	1	0	0	$(0,0,1,1)$	1	$(1,1,1,1)$	1	1
1	1	1	0	1	$(0,1,1,1)$	1	$(1,1,1,1)$	1	1

(5) Let $\omega \in M^{\mathrm{or}}$. The Boolean values for $\omega \in$ (or $\notin$) L, U, L_5, U_2, U_3 coincide.

x	a	y	b	z	list `L`	$\vee$`L` $= \wedge$`U`	list `U`	L_5	U_5
0	1	0	1	0	$(0,0,0,0)$	0	$(1,0,0,1)$	0	1
0	1	0	1	1	$(1,1,0,0)$	1	$(1,1,1,1)$	1	1
1	1	0	1	0	$(0,0,1,1)$	1	$(1,1,1,1)$	1	1
1	1	0	1	1	$(1,1,1,1)$	1	$(1,1,1,1)$	1	1

(6) Let $\omega \in M^{\mathrm{and}}$. The Boolean values for $\omega \in$ (or $\notin$) L, U, U_5, L_2, L_3 coincide.

x	a	y	b	z	list `L`	$\vee$`L` $= \wedge$`U`	list `U`	L_5	U_5
0	0	1	0	0	$(0,0,0,0)$	0	$(0,0,0,0)$	0	0
0	0	1	0	1	$(0,0,0,0)$	0	$(1,0,1,0)$	0	0
1	0	1	0	0	$(0,0,0,0)$	0	$(0,1,0,1)$	0	0
1	0	1	0	1	$(0,1,1,0)$	1	$(1,1,1,1)$	0	1

Remark 5.2. Simple inspection of the tables shows that the Boolean values for L and U coincide in all possible cases, whence a proof of $L = U$ in the power set case. Moreover, one may observe that in all but one cases, L coincides with $L_{23} := L_2 \vee L_3$, resp. with $L_{14} := L_1 \vee L_4$, and in all but one cases, U coincides with $U_{14} := U_1 \wedge U_4$, resp. with $U_{23} := U_2 \wedge U_3$. In all but two cases, L coincides with L_5. Likewise for U and U_5. Also, the rule of defining L and U is rather close to a *majority function* ("the winner takes it all": if ω belongs to at least 3 of the 5 sets, then it belongs to L and to U) – however, 4 among the 32 cases violate this rule.

Coming back to the proof of associativity of the product $(x,z) \mapsto x \bullet z = x \cdot_{a,y,b} z$, direct inspection of the tables shows that, when restricting $\bullet$ to the six subsets from Def. 5.3 , we get in the respective cases:

(1) on M^{true}, $\bullet$ is the "true" connector $(x,z) \mapsto 1_{M^{\mathrm{true}}}$,
(2) on M^{false}, it is the "false" connector $(x,z) \mapsto 0_{M^{\mathrm{false}}}$,
(3) on M^{right}, it is the "second" connector $(x,z) \mapsto z$,
(4) on M^{left}, it is the "first" connector $(x,z) \mapsto x$,
(5) on M^{or}, it is the "or" connector $(x,z) \mapsto x \vee z$,
(6) on M^{and}, it is the "and" connector $(x,z) \mapsto x \wedge z$.

Now, each of the six binary operations listed above obviously is associative.[1] From this it follows that $\bullet$ is also associative: for $i \in I := \{\mathrm{true}, \mathrm{false}, \mathrm{right}, \mathrm{left}, \mathrm{or}, \mathrm{and}\}$, and $x \in \mathcal{P}(M)$, let $x^i := x \cap M^i$, so $x = \sqcup_{i\in I} x^i$ (disjoint union). Then, by what we have just seen, $(x \bullet z)^i = x^i \bullet z^i$ is given by the connector corresponding to i, hence

$$\begin{aligned}(x \bullet w) \bullet z &= \sqcup_{i\in I}((x \bullet w) \bullet z)^i = \sqcup_{i\in I}(x^i \bullet w^i) \bullet z^i \\ &= \sqcup_{i\in I} x^i \bullet (w^i \bullet z^i) = x \bullet (w \bullet z).\end{aligned}$$

Moreover, each of the six connectors has the "weak band property", as is immediately checked, and hence by the same argument, $\bullet$ also is a weak band. Notice also that the opposite product of $\bullet$ is gotten by exchanging a and b (which corresponds

[1] Remarkably, these six products correspond exactly to the six semigroup laws on the set of two elements which are not group laws, and also to the free distributive lattice on 2 generators.

to exchanging the indices “right” and “left” and keeping the other four), which corresponds to the opposite vertex in the “hexad”.

Next, consider the product $L_{(x,a,y)}$. We present the information contained in the precding tables, structured in a different way: fix the Boolean values for $(\omega \in x, \omega \in a, \omega \in y)$ and consider those for $\omega \in L(x,a,y,b,z)$ as a function of those of $(\omega \in b, \omega \in z)$.

1. When ω is in at most one of the sets x, a, y, then we get the “and”-connector:

x	a	y	b	z	$L = U$
0	0	0	0	0	0
0	0	0	0	1	0
0	0	0	1	0	0
0	0	0	1	1	1

x	a	y	b	z	$L = U$
0	0	1	0	0	0
0	0	1	0	1	0
0	0	1	1	0	0
0	0	1	1	1	1

x	a	y	b	z	$L = U$
0	1	0	0	0	0
0	1	0	0	1	0
0	1	0	1	0	0
0	1	0	1	1	1

x	a	y	b	z	$L = U$
1	0	0	0	0	0
1	0	0	0	1	0
1	0	0	1	0	0
1	0	0	1	1	1

2. When $\omega \notin x$ and $\omega \in a \wedge y$, then we get the “left”-connector:

x	a	y	b	z	$L = U$
0	1	1	0	0	0
0	1	1	0	1	0
0	1	1	1	0	1
0	1	1	1	1	1

3. When $\omega \notin a$ and $\omega \in x \wedge y$, then we get the “right”-connector:

x	a	y	b	z	$L = U$
1	0	1	0	0	0
1	0	1	0	1	1
1	0	1	1	0	0
1	0	1	1	1	1

4. When $\omega \in x \wedge a$, then we get the “true” connector:

x	a	y	b	z	$L = U$
1	1	0	0	0	1
1	1	0	0	1	1
1	1	0	1	0	1
1	1	0	1	1	1

x	a	y	b	z	$L = U$
1	1	1	0	0	1
1	1	1	0	1	1
1	1	1	1	0	1
1	1	1	1	1	1

In all four cases, we get a semigroup law satisfying the “weak band” property, and decomposing M into a disjoint union of sets where these properties hold, it follows as above that the product $L_{(x,a,y)}$ has these properties on M. The product $L_{(a,x,y)}$ is the opposite product of $L_{(x,a,y)}$, and hence also has the same properties – note that exchange of (a,x) just exchanges cases 2. and 3. above. Next, fix the Boolean values for $\omega \in x, y, b$ and list those of $\omega \in L(x,a,y,b,z)$ as function of those of $\omega \in (a,z)$. The result is similar as above, in a "dual" way:

(1) When ω is in at most one of $\neg x, \neg b, \neg y$, then we get the "or"-connector.

(2) When $\omega \in x$ and $\omega \in (\neg b \wedge \neg y)$, then we get the "left"-connector.

(3) When $\omega \in b$ and $\omega \in (\neg x \wedge \neg y)$, then we get the "right"-connector.

(4) When $\omega \in (\neg x \wedge \neg b)$, then we get the "false" connector.

As above, this implies the statements of Theorem 5.2 for $L_{(x,y,b)}$ and $L_{(b,y,x)}$, and finishes its proof. □

Definition 5.4. *For each of the products from the "hexad", we call its* bottom *the set corresponding to the "true" connector, and we shall the use the notation* M^{true} *already used for* $\bullet$. *We call its* top *the set corresponding to the "false" connector, and we shall use the notation* M^{false} *already used for* $\bullet$. *Thus, for all* $u, v \in \mathcal{X}$,

$$M^{\mathrm{true}} \leq u \cdot v \leq (M \setminus M^{\mathrm{false}}) = \neg M^{\mathrm{false}}.$$

Theorem 5.5. *Let* $\mathcal{X} = \mathcal{P}(M)$ *be the lattice of the power set of a set* M. *For the six products from the hexad, bottom and top are given by*

(1) for $\bullet = L_{(a,y,b)}$, *we have* $M^{\mathrm{true}} = a \wedge y \wedge b$ *and* $M^{\mathrm{false}} = \neg(a \vee y \vee b)$,

(2) for $L_{(x,a,y)}$, *we have* $M^{\mathrm{true}} = x \wedge a$, *and* $M^{\mathrm{false}} = \emptyset$,

(3) for $L_{(x,y,b)}$, *we have* $M^{\mathrm{false}} = (\neg x \wedge \neg b) = \neg(x \vee b)$, *and* $M^{\mathrm{true}} = \emptyset$,

(4) products belonging to opposite hexad vertices have same bottom and top.

Proof. All statements follow by direct inspection from the tables given above. □

Remark 5.3. We'll see in the arithmetic case that the existence of a non-empty bottom causes a certain *square periodicity* of the respective products. More precisely, there may also be a *periodicity in a single argument*, related to the following result.

Theorem 5.6. *Let* $\mathcal{X} = \mathcal{P}(M)$ *be the lattice of the power set of a set* M. *Fix a triple* $(a,y,b) \in \mathcal{X}^3$. *Then the principal product* $x \bullet z = x \cdot_{a,y,b} z$ *is*

(1) $a \wedge y$-periodic *in* x, *i.e., for all* x *and* z: $\quad (x \vee (a \wedge y)) \bullet z = x \bullet z$,

(2) $b \wedge y$-periodic in z, *i.e., for all* x *and* z: $\quad x \bullet z = x \bullet (z \vee (b \wedge y))$.

Proof. Claim (1) amounts so saying that $L' = L(x \vee (a \wedge y), a, y, b, z)$ and $L = L(x,a,y,b,z)$ have same Boolean values for $\omega \in M$. Now, looking at the tables of Boolean values describing $\bullet$, the cases $\omega \in a \wedge y$ correspond to M^{true} (where L' and L both always have value 1), and M^{left} (containing two lines which are distinguished only by one entry, corresponding to the periodicity claim). Likewise for Claim (2). □

Ternary products. – In certain contexts it is useful to switch the viewpoint from *binary* to *ternary* products, e.g., when looking at the "affine analog" of groups, which have been called *torsor* in [BeKi10a]. Fix a pair $(a,b) \in \mathcal{X}^2$, and consider the remaining *three* arguments (x,y,z) as variables, i.e., we define a *ternary product*

$$\mathcal{X}^3 \to \mathcal{X}, \quad (x,y,z) \mapsto (xyz)_{ab} := L(x,a,y,b,z) = x \cdot_{a,y,b} z. \tag{5.2}$$

Theorem 5.7. *Let $\mathcal{X}$ be a bounded distributive lattice, and fix $(a,b) \in \mathcal{X}^2$. Then:*

(1) the product (5.2) *is* associative *and* para-associative*: $\forall x, x', y, z, z' \in \mathcal{X}$,*

$$((xx'y)_{ab}z'z)_{ab} = (x(x'yz')_{ab}z)_{ab}$$
$$= (x(z'yx')_{ab}z)_{ab} = (xx'(yz'z)_{ab})_{ab},$$

(2) the "middle" operator $M_{x,z}(y) := (xyz)_{ab}$ is idempotent; more precisely,

$$M_{x,z} \circ M_{x,z} = M_{x,z} = M_{x,z} \circ M_{z,x}.$$

Proof. (1) As for the binary products, it suffices to prove the theorem for $\mathcal{X} = \mathcal{P}(M)$, a power set lattice. With respect to the fixed pair (a,b), we decompose M into the disjoint union of four subsets, using notation from Def. 5.3,

$$M = \big(M^{\mathrm{true}} \sqcup M^{\mathrm{and}}\big) \sqcup \big(M^{\mathrm{false}} \sqcup M^{\mathrm{or}}\big) \sqcup M^{\mathrm{right}} \sqcup M^{\mathrm{left}}.$$

Then, as is seen directly from the tables describing the Boolean values of $\bullet$, the ternary map $(x,y,z) \mapsto (xyz)_{ab} := L(x,a,y,b,z)$ coincides with

$(x,y,z) \mapsto x \wedge y \wedge z$ on the first set $M^{\mathrm{true}} \sqcup M^{\mathrm{and}}$,
$(x,y,z) \mapsto x \vee y \vee z$ on the second set $M^{\mathrm{false}} \sqcup M^{\mathrm{or}}$,
$(x,y,z) \mapsto z$ on the third set M^{right} ,
$(x,y,z) \mapsto x$ on the fourth set M^{left}.

Thus the ternary product $(xyz)_{ab}$ will inherit properties that are in common for these four elementary ones. Now, it is immediately checked that all four "elementary" ternary products are associative and para-associative, whence (1). Concerning (2), it is clear that in all four cases middle multiplication operators are idempotent. Eg., for the right product $(xyz) = z$, we get $(x(xyz)z) = (xzz) = z = (xyz)$ and $(x(zyx)z) = (xxz) = z = (xyz)$. □

Remark 5.4. There is no "hexad" of ternary products: the preceding result does not carry over to the other "parastrophe" ternary products.

6. The arithmetic case

6.1. **Comparison with the Boolean case, and general results.** Now consider the possibly most interesting distributive lattice, the lattice $\mathcal{X} = \mathbb{N}_0$ of natural numbers with $\wedge = \mathrm{lcm}$ and $\vee = \mathrm{gcd}$. Via the *p-adic valuation* $n \mapsto v_p(n)$, for each prime number p, transforming the lattice operations to min and max,

$$v_p(\mathrm{lcm}(x,y)) = \max(v_p(x), v_p(y)),$$
$$v_p(\gcd(x,y)) = \min(v_p(x), v_p(y)). \tag{6.1}$$

it is closely related to the *totally ordered case* (Theorem 4.1). This imbedding can also be formulated as an imbedding into a power set $\mathcal{P}(\mathbb{P})$ (Remark 6.1), realizing the arithmetic case as a sublattice of a Boolean lattice. However, the arithmetic lattice seems to be "quite far away" from the Boolean case, and has a rather particular flavor.

Remark 6.1. The imbedding of the lattice $(\mathbb{N}_0, \wedge, \vee)$ into a power set lattice can be described directly as follows: let

$$\mathbb{P} := \{p^k \mid p \text{ prime, or } p = 1, \text{ and } k \in \mathbb{N}\} \subset \mathbb{N}, \tag{6.2}$$

the set of prime powers. Assembling the evaluation maps into a single object, let

$$\lambda : \mathbb{N}_0 \to \mathcal{P}(\mathbb{P}), \quad 0 \mapsto \mathbb{P},\, n \mapsto \lambda(n) := \{m \in \mathbb{P} \mid \ m \big| n\}, \tag{6.3}$$

sending n to the set of prime power divisors of n. Note that, with our choice of notation, this version of λ is *antitone* (this is inevitable if we want to denote both intersection of ideals in $\mathbb{Z}$ and of subsets of $\mathbb{P}$ by the same symbol $\wedge$):

$$\lambda(n \wedge m) = \lambda(\mathrm{lcm}(n,m)) = \lambda(n) \cup \lambda(m) = \lambda(n) \vee \lambda(m),$$
$$\lambda(n \vee m) = \lambda(\mathrm{gcd}(n,m)) = \lambda(n) \cap \lambda(m) = \lambda(n) \wedge \lambda(m).$$

Using this imbedding, we can complete $\mathbb{N}_0$ to a Boolean algebra, adding the missing complement map, simply by taking the sublattice $\mathcal{X}(\mathbb{N}_0) \subset \mathcal{P}(\mathbb{P})$ generated by $\lambda(\mathbb{N}_0)$ and all complement sets $\overline{n} := \neg(\lambda(n))$ for $n \in \mathbb{N}_0$. It is quite easy to see that $\mathcal{X}(\mathbb{N}_0) = \mathcal{P}^{\mathrm{fin}}(\mathbb{P}) \sqcup \mathcal{P}^{\mathrm{cof}}(\mathbb{P})$ is precisely the *finite-cofinite algebra of* $\mathbb{P}$, i.e., the union of the collection of all *finite* subsets of $\mathbb{P}$ and all *cofinite* subsets of $\mathbb{P}$. Being a Boolean algebra, it is stable under U and L.

Definition 6.1. *For a fixed triple $(a,y,b) \in \mathbb{N}^3$, we call*

$n = n_{y,b} := \mathrm{lcm}(y,b)$ *"line period",*
$m := m_{y,a} := \mathrm{lcm}(y,a)$ *"column period",*
$N := N_{a,y,b} := \mathrm{lcm}(a,y,b)$ *"square period" (bottom),*
$K := K_{a,y,b} := \mathrm{gcd}(a,y,b)$ *"base frequency" (top).*

We shall mostly be interested in the "principal products" $\bullet_{a,y,b}$. When $N = 0$, then its description follows directly from Theorem 2.2:

Theorem 6.2. *Let $(a,y,b) \in \mathbb{N}_0^3$ such that $N = 0$. Then,*

(1) if $y = 0$, we have $x \bullet_{a,0,b} z = L_5(x,a,y,b,z) = (b \wedge z) \vee (a \wedge x)$,
(2) if $a = 0$, we have $x \bullet_{0,y,b} z = L_2(x,a,y,b,z) = z \wedge (b \vee (x \wedge y))$,
(3) if $b = 0$, we have $x \bullet_{a,y,0} z = L_3(x,a,y,b,z) = x \wedge (a \vee (z \wedge y))$.

In particular, we have

(1) $x \bullet_{1,0,1} z = x \vee z$,
(2) $x \bullet_{0,1,0} z = x \wedge z$,
(3) $x \bullet_{1,0,0} z = x = x \bullet_{1,1,0} z = z \bullet_{0,1,1} x = z \bullet_{0,0,1} x$.

Definition 6.3. *Let $(a,y,b) \in \mathbb{N}^3$ (so $N \neq 0$ and $K \neq 0$), let $[1, KN]$ be the set of divisors of KN. For $x \in [1, KN]$, we call $x' := \frac{KN}{x}$ its* conjugate divisor*, and define the* conjugate product

$$\mathbb{N}_0^2 \to \mathbb{N}_0, \quad (x,z) \mapsto x \bullet_{b',y',a'} z.$$

Theorem 6.4. *Let $(a,y,b) \in \mathbb{N}_0^3$ such that $N \neq 0$. Then:*

(1) For all $(x,z) \in \mathbb{N}_0^2$, $L(x,a,y,b,z)$ belongs to the set of divisors of N, and is a multiple of K. In particular, $x \bullet_{a,y,b} z$ takes only a finite number of values.
*(2) The product $\bullet_{a,y,b}$ is (n,m)-*periodic *in the following sense:*

$$x \equiv x' \mathrm{mod}(n) \quad \Rightarrow \quad x \bullet_{a,y,b} z = x' \bullet_{a,y,b} z,$$
$$z \equiv z' \mathrm{mod}(m) \quad \Rightarrow \quad x \bullet_{a,y,b} z = x \bullet_{a,y,b} z'.$$

It follows that the product $\bullet_{a,y,b}$ passes to the quotient defining a product on $\mathbb{Z}/N\mathbb{Z}$, or even on $K\mathbb{Z}/N\mathbb{Z}$.

(3) The "conjugation map"

$$\gamma : [1, KN] \to [1, KN], \quad x \mapsto x' = \frac{KN}{x}$$

is an isomorphism from the semigroup $[1, KN]$ *with product* $\bullet_{a,y,b}$ *onto the semigrop* $[1, KN]$ *with conjugate product* $\bullet_{b',y',b'}$*. By restriction, the same holds for the subsemigroup* $[K, N] = \{d \mid K|d, \ d|N\}$*.*

Proof. (1) and (2) are a reformulation of parts of Theorems 5.2, 5.5, and 5.6.

(3) Clearly, γ is a lattice involution (antiautomorphism of order 2) of the lattice $[1, KN]$ (cf. Example 3.1). The claim now follows from Lemma 2.4. □

Remark 6.2. The isomorphism from item (3) does not directly extend to an isomorphism $(\mathbb{N}_0, \bullet_{a,y,b}) \to (\mathbb{N}_0, \bullet_{a',y',b'})$. Rather than "isomorphic", these products are "isotopic", in the sense that when imbedding $\mathbb{N}_0$ into a Boolean algebra (Remark 6.1), then both products are the "same", but evaluated on "opposite" copies of $\mathbb{N}_0$.

6.2. **Examples of tables.**

Remark 6.3. The reader may enjoy to do some numerical tests herself. Here is the program which we have used for computing L and U in the following tables, along with L_i, U_i, for $i = 1, \dots, 4$, by using SageMath, along with a random example:

```
def Bounds(x,a,y,b,z):
L=[lcm(b,gcd(z,lcm(a,y))), lcm(z,gcd(b,lcm(x,y))),
   lcm(x,gcd(a,lcm(z,y))), lcm(a,gcd(x,lcm(b,y)))] ;
U=[gcd(a,lcm(z,gcd(y,b))), gcd(x,lcm(b,gcd(z,y))),
   gcd(z,lcm(a,gcd(x,y))), gcd(b,lcm(x,gcd(a,y)))] ;
print(L) ; print(gcd(L)) ;
print(U) ; print(lcm(U))
```

```
Bounds(425, 204, 1000, 200, 402)     Bounds(425, 200, 1000, 204, 402)
[600, 40200, 5100, 5100] 300         [204, 13668, 3400, 3400] 68
[12, 25, 6, 100] 300                 [4, 17, 2, 68] 68
```

Now let us write up some "multiplication tables" for fixed (a, y, b). By Theorem 2.2, the left upper corner of all of the following multiplication tables (first column: values x, first line: values z) is given by

$$\begin{aligned}
&0 \bullet_{a,y,b} 0 = a \wedge y \wedge b = N \text{ (the square period)}, \\
&0 \bullet_{a,y,b} 1 = b, \\
&1 \bullet_{a,y,b} 0 = a, \\
&1 \bullet_{a,y,b} 1 = a \vee y \vee b = K \text{ (the base frequency)}.
\end{aligned}$$

Also by Theorem 2.2, when $a = b$, then a always is an *absorbing element* (taking the role of the zero element in usual quotient rings): $\forall x \in \mathbb{N}$,

$$a \bullet_{a,y,a} x = L(a, a, y, a, x) = a = x \bullet_{a,y,a} a.$$

In particular, when $a = y = b$, then $x \bullet_{a,a,a} z = a$.

Example 6.1. The multiplication table for $x \bullet_{1y1} z = x \vee y \vee z$ is y-periodic; if y is a prime number, it takes two values; e.g., for $y = 2$:

$x \bullet_{1,2,1} z$	0	1	2	3	4	5
0	2	1	2	1	2	1
1	1	1	1	1	1	1
2	2	1	2	1	2	1

When $y = 8$, the extracted table for the divisors of $N = 8$ is a "minimum-law":

$x \bullet_{1,8,1} z$	1	2	4	8
1	1	1	1	1
2	1	2	2	2
4	1	2	4	4
8	1	2	4	8

Example 6.2 (Prime power cases). These are the cases where p is a prime number and $(a, y, b) = (p^k, p^\ell, p^m)$ with $k, \ell, m \in \mathbb{N}_0$. For instance:

$x \bullet_{8,4,2} z$	0	1	2	3	4	5	6	7	8
0	8	2	2	2	4	2	2	2	8
1	8	2	2	2	4	2	2	2	8
2	8	2	2	2	4	2	2	2	8

One observes an effective line period 1, instead of the predicted $n = 4$. Indeed, it follows from Theorem 4.1 that $x \cdot_{8,4,2} z = 2^{\max(1,\min(v_p(z),3))}$, which does not depend on x. In the prime power case, $x \cdot_{a,y,b} z$ is solely determined by the p-adic valuation $v_p(x), v_p(z)$ of x and z and the L- and U-functions for a totally ordered set (Theorem 4.1). The cases $k \geq \ell \geq m$ and $k \leq \ell \leq m$ behave like the preceding example. The other cases are more complicated. For instance, here is the table for the divisors of 16 with $(a, y, b) = (8, 1, 16)$:

$x \bullet_{8,1,16} z$	1	2	4	8	16
1	1	2	4	8	8
2	2	2	4	8	8
4	4	4	4	8	8
8	8	8	8	8	8
16	16	16	16	16	16

When $(a, y, b) = (8, 1, 8)$, the extracted table is similar: just skip the last line and the last column of the preceding table. Note that we get the table of a "maximum-law", which is "dual" to the corresponding table of the conjugate product $(1, 8, 1)$.

Example 6.3. When $(a, y, b) = (p, 1, q)$ with p, q two prime numbers, then the structure of the products $x \bullet_{p,1,q} z = (p \vee x) \wedge (q \vee z)$ follows this pattern:

$x \bullet_{5,1,3} z$	0	1	2	3	4	5
0	15	3	3	3	3	15
1	5	1	1	1	1	5
2	5	1	1	1	1	5
3	15	3	3	3	3	15

The extracted table for the divisors of 15 is

$x \bullet_{5,1,3} z$	1	3	5	15
1	1	1	5	5
3	3	3	15	15
5	1	1	5	5
15	3	3	15	15

which agrees with the "dual" table of divisors of 15 for $(5, 15, 3)$.

Example 6.4. Let $y = 2$. First the table for the commutative product $\bullet_{3,2,3}$, having line and column period 3 and square period 6. The element 3 is absorbing (constant line and column 3).

$x \bullet_{3,2,3} z$	0	1	2	3	4	5	6
0	6	3	6	3	6	3	6
1	3	1	1	3	1	1	3
2	6	1	2	3	2	1	6
3	3	3	3	3	3	3	3
4	6	1	2	3	2	1	6
5	3	1	1	3	1	1	3
6	6	3	6	3	6	3	6

The table for the non-commutative product $\cdot_{3,2,4}$ having line period 4 and column period 6 and square period 12 has been given in the introduction. As it turns out, there is an even shorter period 3 concerning columns.

Next, the table for the non-commutative product $\cdot_{3,2,5}$ having line period 10 and column period 6 and square period 30:

$x \cdot_{3,2,5} z$	0	1	2	3	4	5	6
0	30	5	10	15	10	5	30
1	3	1	1	3	1	1	3
2	6	1	2	3	2	1	6
3	3	1	1	3	1	1	3
4	6	1	2	3	2	1	6
5	15	5	5	15	5	5	15
6	6	1	2	3	2	1	6
7	3	1	1	3	1	1	3
8	6	1	2	3	2	1	6
9	3	1	1	3	1	1	3
10	30	5	10	15	10	5	30

The same table gives rise to the multiplication table for the set of divisors of 30:

$x \cdot_{3,2,5} z$	1	2	3	5	6	10	15	30
1	1	1	3	1	3	1	3	3
2	1	2	3	1	6	2	3	6
3	1	1	3	1	3	1	3	3
5	5	5	15	5	15	5	15	15
6	1	2	3	1	6	2	3	6
10	5	10	15	5	30	10	15	30
15	5	5	15	5	15	5	15	15
30	5	10	15	5	30	10	15	30

Example 6.5. Here an example where a, y, b are composed numbers having common factors:

$x \cdot_{2,6,3} z$	0	1	2	3	4	5
0	6	3	6	3	6	3
1	2	1	2	1	2	1
2	2	1	2	1	2	1
3	6	3	6	3	6	3
4	2	1	2	1	2	1
5	2	1	2	1	2	1

and the extracted table for the divisors of 6 is:

$x \cdot_{2,6,3} z$	1	2	3	6
1	1	2	1	2
2	1	2	1	2
3	3	6	3	6
6	3	6	3	6

When a, y, b have all three non-trivial factors in common, the structure of the products becomes quite complicated, and certainly deserves to be studied further.

Example 6.6. Recall from Theorem 5.5 that the non-principal parastrophes may have a "bottom", or not. When the bottom is empty, then the tables are non-periodic. This is the case, for instance, for the product $(a, z) \mapsto L(8, a, 4, 2, z)$:

$a \backslash z$	0	1	2	3	4	5	6	7	8
0	0	2	2	6	4	10	6	14	8
1	4	2	2	2	4	2	2	2	4
2	4	2	2	2	4	2	2	2	4
3	12	2	2	6	4	2	6	2	4
4	4	2	2	2	4	2	2	2	4
5	20	2	2	2	4	10	2	2	4
6	12	2	2	4	6	2	6	2	4
7	28	2	2	2	4	2	2	14	4

There is no easily visible pattern how to continue this table. The parastrophic product $(b, z) \mapsto L(8, 2, 4, b, z)$ is periodic and seems to follow a pattern similar to a "principal" product:

$b \backslash z$	0	1	2	3	4	5	6	7	8
0	8	8	8	8	8	8	8	8	8
1	4	1	2	1	4	1	2	1	4
2	4	2	2	2	4	2	2	2	4
3	4	1	2	1	4	1	2	1	4
4	4	4	4	4	4	4	4	4	4
5	4	1	2	1	4	1	2	1	4
6	4	2	2	2	4	2	2	2	4
7	4	1	2	1	4	1	2	1	4
8	8	8	8	8	8	8	8	8	8

These constructions give a considerable number of finite semigroups, and hence seem to be a quite effective machinery to "produce" semigroups.

7. Afterthoughts

In several respects, the arithmetic case is an "antipode" of the geometric approach developed in [BeKi10a, BeKi10b, BeKi12]. Namely, from a geometric point of view, the arithmetic case is a "zero dimensional projective geometry": if $\mathbb{K}$ is a field, then $\mathrm{Gras}_{\mathbb{K}}(\mathbb{K})$ would be the zero-dimensional projective space $\mathbb{K}\mathbb{P}^0$, which is uninteresting. If $\mathbb{K}$ is a ring, notably, for $\mathbb{K} = \mathbb{Z}$, things change considerably:

(1) *transversality* is a major tool used in [BeKi10a]; but the arithmetic case does not admit any transversal pairs (two non-trivial submodules of $\mathbb{Z}$ always have non-trivial intersection)!
(2) *anti-automorphisms* are crucial ingredients to define "classical geometries" (see [BeKi10b]), but in the arithmetic case there are no antiautomorphisms,
(3) of course, one can define abstractly a "dual geometry" (just by taking the dual lattice and exchanging a and b); but at a first glance there is no "natural model" how to "realize this dual geometry in nature",
(4) *group actions with "big" ("open") orbits* are heavily used in [BeKi10a]; but in the arithmetic case, the geometry is *highly non-homogeneous*: the linear group $\mathrm{GL}(1,\mathbb{Z}) = \{\pm 1\}$ has trivial orbits in $\mathbb{N}$, and hence group-theoretic arguments are of no use.

Thus, from a geometric viewpoint, the arithmetic case seems to be difficult to understand. As we have seen, this is partially compensated by the simple formula $L = \Gamma = U$; but a deeper understanding of the link between the geometric and the arithmetic aspects would be desirable.

References

[BeKi10a] W. Bertram and M. Kinyon, Associative Geometries. I: Torsors, Linear Relations and Grassmannians, *Journal of Lie Theory* 20 (2) (2010), 215-252; arXiv : https://arxiv.org/abs/0903.5441

[BeKi10b] W. Bertram and M. Kinyon, Associative Geometries. II: Involutions, the classical torsors, and their homotopes, *Journal of Lie Theory* 20 (2) (2010), 253-282; https://arxiv.org/abs/0909.4438

[BeKi12] W. Bertram and M. Kinyon, Torsors and ternary Moufang loops arising in projective geometry. p 343 - 360 in: Algebra, Geometry and Mathematical Physics, Springer-Verlag 2014 (Proceedings of the AGMP, Mulhouse, France, October 2011) http://arxiv.org/abs/1206.2222

[Be12] W. Bertram, The projective geometry of a group, http://arxiv.org/abs/1201.6201

[Be14] W. Bertram, Universal Associative Geometry. http://arxiv.org/abs/1406.1692

[Bi] Birkhoff, G., *Lattice Theory*, AMS Colloquium Publications XXV, (Third edition), Rhode Island 1973

[BS] Burris, S., and H. P. Sankappanavar, *A Course in Universal Algebra*, Springer 1981

[CS03] Conway, J.H., and D.A. Smith, *On quaternions and octonions: their geometry, arithmetic, and symmetry*, A.K. Peters Ltd, Natick MA, 2003.

[S38] Stone, M., "Topological representations of distributive lattices and Brouwerian logics", Czasopis pro postovn matematiky a fysiky, Vol. 67 (1938), No. 1, 1–25

Institut Élie Cartan de Lorraine, Université de Lorraine at Nancy, CNRS, INRIA, Boulevard des Aiguillettes, B.P. 239, F-54506 Vandœuvre-lès-Nancy, France, url: http://iecl.univ-lorraine.fr/~Wolfgang.Bertram/

E-mail address: wolfgang.bertram@univ-lorraine.fr