ARITHMETIC OF LOGIC*

BY
E. T. BELL

1. Introduction. This is probably the first attempt to construct an arithmetic for an algebra of the non-numerical genus.† In his classic treatise, *An Investigation of the Laws of Thought*,‡ Boole developed the thesis that "Logic (is) · · · a system of processes carried on by the aid of symbols having a definite interpretation, and subject to laws founded on that interpretation alone. But at the same time they exhibit those laws as identical in form with the laws of the general symbols of Algebra, with this simple addition, viz., that the symbols of Logic are further subject to a special law, to which the symbols of quantity as such, are not subject." The special law is what Boole calls the law of duality, $x(1-x)=0$, or the excluded middle; here the indicated multiplication is logical, $1-x$ is the supplement of x. Boole showed therefore that abstractly logic is contained in common algebra.

Taking rational arithmetic $\mathfrak{A}$ ($\equiv$ the theory of numbers in reference to the positive rational integers 0, 1, 2, 3, · · · , only) and certain parts of the theory of algebraic numbers, particularly the rudiments of Dedekind's theory of ideals and those of Kronecker's modular systems as our guides, we shall see to what extent Boole's algebra of logic may be *arithmetized* in a precise sense to be defined presently. Although it will be unnecessary to refer explicitly anywhere to the theory of algebraic numbers, it may be mentioned that this theory, which includes rational arithmetic, is a surer guide than the latter in problems of arithmetization. In rational arithmetic the essential abstract structure of the concepts to be extended beyond 0, 1, 2, · · · is often quite ingeniously concealed. This is true, for example, of the G.C.D., L.C.M., and residuation. The theory of ideals, on the other hand, often indicates immediately what transformations by formal equivalence must first be applied to operations or relations of rational arithmetic in order that they shall be significant for sets of elements for which order relations are either irrelevant or meaningless.

---

* Presented to the Society, San Francisco Section, April 2, 1927; received by the editors November 29, 1926.

† For the meaning of this term, cf. Whitehead, *Universal Algebra*, p. 29.

‡ London and Cambridge, 1854; reprinted, Chicago, Open Court, 1916, as vol. 2 of Boole's *Collected Logical Works*.

We shall use a few of the commonest notations of algebraic logic; thus $P \supset Q$ for P *implies* Q; $P :\equiv : Q$ for P, Q, *are formally equivalent*, viz.,

$$P \supset Q. \quad Q \supset P,$$

the dot in the last being the logical *and*; $\equiv$ signifies *definitional identity*, except where it occurs in conjunction with mod, when it indicates congruence, as in $\alpha \equiv \beta \bmod \mu$; the special notation $\alpha | \beta$, borrowed from the theory of numbers, where α, β are *classes*, signifies α *contains* β, $\equiv$ *each element of* β *is in* α. To avoid confusion we shall never use "contains" in relation to arithmetic; conflicting conventions in this respect have already introduced exasperating paradoxes of language into the theory of numbers.

Small Greek letters $\alpha, \beta, \gamma, \cdots$ will always denote classes; $\mathfrak{C}$ is the set of classes discussed; the *null class* is denoted by ω, the *universal class* by ϵ, so that ω, ϵ are the zero, unity of the *algebra of logic* $\mathfrak{L}$. Elements of $\mathfrak{C}$ will be called elements of $\mathfrak{L}$. *Logical* (but not arithmetical) *addition, multiplication of classes* α, β are indicated as usual by $\alpha+\beta$, $\alpha\beta$, and if α is any element of $\mathfrak{L}$, the *supplement* of α is indicated by an accent, α' (instead of the customary bar which is awkward in monotype). Hence α' is the unique* solution of $\alpha+\alpha' = \epsilon$, $\alpha\alpha' = \omega$, where α is any given element of $\mathfrak{L}$. We shall assume a given set $\mathfrak{C}$ of classes and we postulate that if α, β are any elements of $\mathfrak{C}$, then α', $\alpha+\beta$, $\alpha\beta$ are in $\mathfrak{C}$, and, as before, we refer to elements of $\mathfrak{C}$ as elements of $\mathfrak{L}$.

The letters s, p, l, g denote specific operations upon elements of $\mathfrak{L}$, and they are such that (once for all, without further reference) $\alpha t \beta$ for each of $t = s, p, l, g$ is a uniquely determined element of $\mathfrak{L}$; the letters c, d, r denote specific relations such that $\alpha\ t\ \beta$ for each $t = c, d, r$ is uniquely significant in $\mathfrak{L}$. To assist the memory we remark that s, p, l, g, c, d, r may be read *sum, product, least, greatest, congruent, divides, residual*, terms to be defined in the *arithmetic of logic* as opposed to the algebra. The least, greatest here are intended merely to recall classes having with respect to given classes *properties* abstractly identical with those of the G.C.D., L.C.M. with respect to division in $\mathfrak{A}$; these classes g, l are not necessarily the "most" or the "least" inclusive—the rôles with respect to inclusion may be reversed, and g may be either the most or the least inclusive common class of a set, and similarly for l. Hence we shall not use here the names already familiar in Moore's general analysis.

The *zero, unity* in the *arithmetic* of classes will always be denoted by ζ, υ. It will avoid possible confusion if we add that (ζ, υ) are not necessarily equal to (ω, ϵ) respectively.

---

* For proof of unicity cf. Whitehead, *Universal Algebra*, p. 36.

Suppose all the elements, operations and signs of relations, other than the logical constants, are replaced in a set $\mathfrak{T}$ of propositions by marks without significance beyond that implied by the assertion of the propositions (which include the postulates of the set). Call the result, $C(\mathfrak{T})$, the *content* of $\mathfrak{T}$. If in $C(\mathfrak{T})$ it be possible to assign interpretations to the marks, giving $\mathfrak{T}_j$, such that $\mathfrak{T}_j$ is self-consistent and uniquely significant in terms of the interpretation, we shall call $\mathfrak{T}_j$ an *instance* of $C(\mathfrak{T})$. Sets $\mathfrak{T}_j$ $(j=1, 2, \cdots)$ of propositions having the same content will be called *abstractly identical.*

Our object is to find parts $\mathfrak{A}_j$ of rational arithmetic $\mathfrak{A}$ abstractly identical with parts $\mathfrak{L}_j$ of the algebra of classes, hence also with the algebra of relations, and finally with $\mathfrak{L}$.

In such a project the following type of *invariance under formal equivalence* is extremely useful. Let P_j $(j=1, 2, \cdots)$ be propositions of $\mathfrak{T}$ such that $P_1 : \equiv : P_2$. Then the truth-values of $P_1 \supset P_3$, $P_3 \supset P_1$ are identical with those of $P_2 \supset P_3$, $P_3 \supset P_2$. Thus $: \equiv :$ in propositions is abstractly identical with $=$ in common algebra, and in implications a particular proposition may be replaced by any other which is formally equivalent to it. We shall meet several instances of such transformations which are considerably less obvious than the logic which justifies them. The identical transformation of a set of transformations by formal equivalence is that which replaces each proposition of a given set by itself; any set of transformed propositions (including the set transformed by the identical transformation) is called a *transform* of the original set.

Let $\mathfrak{T}'$ be a transform of $\mathfrak{T}$, and $\mathfrak{A}_j'$ a transform of a part $\mathfrak{A}_j$ of $\mathfrak{A}$. Then if $\mathfrak{T}'$, $\mathfrak{A}_j'$ are abstractly identical, we shall say that $\mathfrak{T}$ is *arithmetized with respect to* $\mathfrak{A}_j$, or simply *arithmetized.*

This kind of arithmetization can be carried much farther for $\mathfrak{L}$ than is done here, but what is given will suffice to show its nature, and it will be evident that at nearly every stage there are alternative ways of proceeding. We shall exhibit arithmetizations of $\mathfrak{L}$ with respect to congruences, the L.C.M., G.C.D., divisibility, primes, and the unique factorization law.

Rational arithmetic $\mathfrak{A}$ presupposes the existence of a special ring. In the whole discussion we shall ignore negative numbers, without loss of generality, as the arithmetic (properties of integers as such) which refers to these can always be thrown back to relations between positive integers only, e.g., as done by Kronecker.

An *abstract ring* $\mathfrak{R}$ is a set $\mathfrak{S}$ of elements $x, y, z, \cdots, u', z', \cdots$, and two operations $S, P(\equiv$ *addition, multiplication*$)$ which may be performed upon any two equal or distinct elements x, y of $\mathfrak{R}$, in this order, to produce uniquely determined elements xSy, xPy such that the postulates $\mathfrak{R}_j$ $(j=1, 2, 3)$ are satisfied. Elements of $\mathfrak{S}$ will be called elements of $\mathfrak{R}$.

$\mathfrak{R}_1$. If x, y are any two elements of $\mathfrak{R}$, xSy, xPy are uniquely determined elements of $\mathfrak{R}$, and

$$ySx = xSy, \qquad yPx = xPy.$$

$\mathfrak{R}_2$. If x, y, z are any three elements of $\mathfrak{R}$,

$$(xSy)Sz = xS(ySz), \qquad (xPy)Pz = xP(yPz),$$
$$xP(ySz) = (xPy)S(xPz).$$

$\mathfrak{R}_3$. There exist in $\mathfrak{R}$ two distinct* unique elements, denoted by u', z', and called the *unity, zero* of $\mathfrak{R}$, such that if x is any element of $\mathfrak{R}$, $xSz' = x$, $xPu' = x$.

These may be compared with the first three postulates of Dickson† for a field, of which they are a transcription, except that the unicity of u', z' is here a postulate, not a theorem, also with Wedderburn's‡ for algebraic fields. In each comparison the omissions are to be particularly noticed. Thus in $\mathfrak{R}$ we can *not* infer $x = y$ from $xPz = yPz$ (this inference is in general false for the special rings $\mathfrak{R}'$ considered later), nor does P have a unique inverse, although we shall later define division. The inference $x = y$ from $xSz = ySz$ also is illegitimate. No attempt has been made in defining $\mathfrak{R}$ to achieve conformity with other definitions of rings; we are concerned only with isolating from fields what is useful for our project.

If S, P and the elements of $\mathfrak{R}$ are specialized by interpretation or by the adjunction to $\mathfrak{R}_j$ $(j = 1, 2, 3)$ of further postulates consistent with those for $\mathfrak{R}$, or by both of these restrictions, we shall call the result, $\mathfrak{R}'$, a *special ring*. An instance of $\mathfrak{R}$ is $\mathfrak{A}$.

2. **Algebraic congruence in $\mathfrak{L}$.** Let xCy be a relation in $\mathfrak{R}$ such that, if x, y, z, w are any elements of $\mathfrak{R}$, xCy is uniquely significant in $\mathfrak{R}$ and the postulates (1.1)–(1.4) are satisfied:

(1.1) $\qquad xCy \supset yCx.$

(1.2) $\qquad xCy \;.\; yCz : \supset : xCz.$

(1.3) $\qquad xCy \;.\; zCw : \supset : (xSz)C(ySw).$

(1.4) $\qquad xCy \;.\; zCw : \supset : (xPz)C(yPw).$

Then C is called *abstract algebraic congruence.*

---

* For the theorem, required later, that ζ, υ are distinct, cf. *Principia Mathematica*, 1st edition, p. 231, *24.1. It will not be necessary hereafter to prove that $\mathfrak{L}_j$ is an instance of $\mathfrak{R}$, as $\zeta \neq \upsilon$ is the only proposition not immediately obvious from the definitions.

† *Algebras and their Arithmetics*, p. 201.

‡ Annals of Mathematics, (2), vol. 24 (1923), pp. 237–264, especially p. 240.

If $\mathfrak{R}$ is replaced by its instance $\mathfrak{A}$, an instance of xCy is $aCb \equiv (a \equiv b \bmod m)$, where a, b are integers $\geqq 0$ and m is an integer >0.

In $\mathfrak{A}$ we shall say that C is *arithmetic congruence* if to the instances in $\mathfrak{A}$ of (1.1)–(1.4) be adjoined the three further postulates

$$(1.5) \qquad (a \equiv 0 \mod m) :\equiv : m \text{ divides } a, m \neq 0 ;$$

$$(1.6) \qquad (ka \equiv kb \mod m) \supset (a \equiv b \mod m'), \ m \neq 0,$$

where $qm' = m$, and $q =$ the G.C.D. of k, m;

$$(1.7) \qquad a \equiv a \bmod m.$$

Any set of propositions in $\mathfrak{L}$ abstractly identical with any transform of (1.1)–(1.7) will, if true, be said to define *arithmetic congruence c in* $\mathfrak{L}$.

As a practical detail we assign by convention the truth value (+) (≡true) to an asserted proposition, as for example any instance of (1.1), unless it be expressly noted that the value is (−) (≡false). This merely avoids the repeated assertion that our propositions as stated are (+), which they are.

We shall now proceed to the partial determination of c by solving (1.1)–(1.4) in $\mathfrak{L}$; the discussion in $\mathfrak{L}$ of (1.5), (1.6) must be deferred until after that of the G.C.D. and the residual in $\mathfrak{L}$.

By (1.1) C is symmetric. The only symmetric functions of two classes α, β are (by the laws of tautology and absorption)

$$(2.1) \qquad \alpha\beta, \ \alpha + \beta \text{ and their supplements}$$

$$(2.2) \qquad \alpha' + \beta', \ \alpha'\beta' ;$$

$$(2.3) \qquad \alpha'\beta + \alpha\beta' \text{ and its supplement}$$

$$(2.4) \qquad \alpha\beta + \alpha'\beta'.$$

The function (2.3) is that which Daniell* has denoted by $|\alpha - \beta|$ and called the *modular difference* of α, β. This is the naturally suggested function for the solution of our problem. It is interesting therefore that it should be rejected by the mildest of the postulates on C, as may be verified in the same way as done presently for another rejection.

Now, by evident analogies between $\mathfrak{L}$ and the theory of division for Dedekind ideals, also by the concept of congruence with respect to an ideal modulus, and further by the "contains" of Kronecker's modular theory, it is immediately suggested that we introduce an arbitrary class μ, constant in (1.1)–(1.4), and seek inclusion relations between μ and each of the symmetric functions σ in (2.1)–(2.4) to satisfy (1.1)–(1.4).

* Bulletin of the American Mathematical Society, vol. 23 (1916), pp. 446–450.

The only inclusion relations for two classes γ, δ are $\gamma|\delta$, $\gamma \neq \omega$ if $\delta \neq \omega$, and $\delta|\gamma$, $\gamma \neq \epsilon$ if $\delta \neq \epsilon$. We therefore test for each σ the truth of the propositions $\sigma|\mu$, $\mu|\sigma$, either of which may turn out to be (+) or (−). It will be sufficient to attend to (2.1) for brevity. Hence we are to test these propositions for (3.1)–(3.4), the truth values being unknown,

(3.1) $\alpha C\beta \equiv \mu \,|\, \alpha\beta$, $\quad \mu \neq \omega$ if $\alpha\beta \neq \omega$,

(3.2) $\alpha C\beta \equiv \alpha\beta \,|\, \mu$, $\quad \mu \neq \epsilon$ if $\alpha\beta \neq \epsilon$,

(3.3) $\alpha C\beta \equiv (\alpha + \beta) \,|\, \mu$, $\quad \mu \neq \epsilon$ if $\alpha + \beta \neq \epsilon$,

(3.4) $\alpha C\beta \equiv \mu \,|\, (\alpha + \beta)$, $\quad \mu \neq \omega$ if $\alpha + \beta \neq \omega$.

The conclusions are summarized in the following table.

	(1.1)	(1.2)	(1.3)	(1.4)
(3.1)	(+)	(−)	(−)	(+)
(3.2)	(+)	(+)	(+)	(+)
(3.3)	(+)	(−)	(+)	(−)
(3.4)	(+)	(+)	(+)	(+)

It will suffice to verify the row (3.2) and check the falsity of one (−) proposition, say (3.1).(1.3), deferring consideration of the exceptions.

From (3.2) we have $\alpha C\beta \equiv \alpha\beta|\mu$, and (1.1) is (+), as it must be automatically since $\alpha\beta$ is symmetric. For (1.2) in this case we should have (+) for

$$\alpha\beta \,|\, \mu \,.\, \beta\gamma \,|\, \mu : \supset : \alpha\gamma \,|\, \mu.$$

Now (cf. Whitehead, loc. cit., p. 43, prop. 14)

$$\alpha \,|\, \beta \,.\, \gamma \,|\, \delta : \supset : \alpha\gamma \,|\, \beta\delta \;;$$

hence

$$\alpha\beta \,|\, \mu \,.\, \beta\gamma \,|\, \mu : \supset : \alpha\beta\beta\gamma \,|\, \mu\mu,$$
$$: \supset : \alpha\beta\gamma \,|\, \mu \;;$$

but $\alpha\gamma|\alpha\beta\gamma$; hence $\alpha\gamma|\mu$. Again, (1.3) requires

$$\alpha\beta \,|\, \mu \,.\, \gamma\delta \,|\, \mu : \supset : (\alpha + \gamma)(\beta + \delta) \,|\, \mu,$$

which is (+), since

$$(\alpha + \gamma)(\beta + \delta) \,|\, \alpha\beta \,.\, (\alpha + \gamma)(\beta + \delta) \,|\, \gamma\delta \;;$$

and (1.4) in this case is

$$\alpha\beta \,|\, \mu \,.\, \gamma\delta \,|\, \mu : \supset : \alpha\beta\gamma\delta \,|\, \mu$$

which obviously is (+).

Taking the false (3.1).(1.3) we have $\alpha C\beta \equiv \mu \mid \alpha\beta$, and (1.3) demands

$$\mu \mid \alpha\beta .\ \mu \mid \gamma\delta : \supset : \mu \mid (\alpha + \gamma)(\beta + \delta)$$

which clearly is $(-)$. Similarly for the rest of the table.

Hence we have the alternative *solutions in* $\mathfrak{L}$ *for the problem of algebraic congruence of classes,*

$$(4.1) \qquad (\alpha \equiv \beta \bmod \mu) : \equiv : \alpha\beta \mid \mu, \qquad \mu \neq \epsilon,$$

$$(4.2) \qquad (\alpha \equiv \beta \bmod \mu) : \equiv : \mu \mid (\alpha + \beta), \qquad \mu \neq \omega,$$

and evidently either solution can be inferred from the other by the Peirce-Schröder dualism in $\mathfrak{L}$, viz., the reciprocity between logical addition and multiplication. The values of μ which must be excepted in (4.1), (4.2) will be seen later to be abstractly identical with the excepted modulus zero in $\mathfrak{A}$; in each case the *arithmetic* zero ζ is barred as a modulus μ.

Each problem in $\mathfrak{L}$ has a similar two-valued solution. It is economical however to state both duals in each instance in order to decide readily which must be paired from one solution with one from another to yield the required arithmetic applicable to the simultaneous solutions of several postulate systems.

3. **The transform of reflexiveness of congruence.** Examining the solutions (4.1), (4.2) we see that each violates the simplest property of congruence in $\mathfrak{A}$, viz., *reflexiveness*. For in $\mathfrak{A}$ we have the $(+)$ proposition (1.7) $\equiv$ (5.1),

$$(5.1) \qquad a \equiv a \bmod m,$$

for all elements $a \geqq 0$ of $\mathfrak{A}$ and $m > 0$. But in $\mathfrak{A}$ we have $a - a = 0$. Hence we may replace (5.1) by

$$(5.2) \qquad 0 \equiv 0 \bmod m,$$

since in $\mathfrak{A}$,

$$(0 \equiv 0 \bmod m) : \equiv : (a \equiv a \bmod m).$$

Hence, comparing (5.2), (1.5), we may replace (5.1) by its transform (5.2), and hence *reflexiveness of congruence in* $\mathfrak{A}$ *may be replaced by the proposition that the zero,* 0, *in* $\mathfrak{A}$ *is divisible by every element of* $\mathfrak{A}$, *with the possible exception* (*removed presently*) *of* "0 *divides* 0."

In $\mathfrak{A}$ we either do not define division by zero, in which case dividends with zero divisors are not in our universe of discourse, or we define division by zero, saying that the quotient is wholly indeterminate, and exclude the process. It is impossible to reconcile either procedure with $\mathfrak{L}$, as will be clear when we come to division in $\mathfrak{L}$, so we make a slight compromise which affects

nothing in $\mathfrak{A}$ but which is necessary in $\mathfrak{L}$. We shall exclude division by zero in $\mathfrak{A}$ except in the one case where the dividend is also zero, and we shall say that in this case the quotient exists but is wholly indeterminate.

4. **Division in $\mathfrak{L}$.** Consider in the abstract ring $\mathfrak{R}$ a relation having the properties

$$xDx, \tag{6.1}$$

$$xDy \,.\, yDz : \supset : xDz, \tag{6.2}$$

$$xDy \,.\, yDx : \supset : x = y, \tag{6.3}$$

where xDy is uniquely significant for each $x \neq z'$ (the zero in $\mathfrak{R}$) and y in $\mathfrak{R}$, with the exception (cf. § 3) that $z'Dz'$ is significant but indeterminate in $\mathfrak{R}$.

These are satisfied in $\mathfrak{A}$ by taking $xDy \equiv x$ *divides* y, and they may be (+) in any instance $\mathfrak{R}'$ of $\mathfrak{R}$ irrespective of whether division yields a unique quotient.* In $\mathfrak{L}$ we shall select a solution which does not give a unique quotient but which does lead to a unique factorization theorem—a rather unexpected situation.

As before, analogy with the theory of ideals suggests that we take in $\mathfrak{L}$ an inclusive relation for D. We shall consider both of

$$\alpha D\beta \equiv \alpha \mid \beta, \tag{7.1}$$

$$\alpha D\beta \equiv \beta \mid \alpha, \tag{7.2}$$

as definitions (in different interpretations) of *algebraic division in* $\mathfrak{L}$. We may read (7.1) as α *divides* β, *or* β *is a multiple of* α, *is identical with* α *contains* β; (7.2) is read α *divides* β, *or* β *is a multiple of* α, *is identical with* β *contains* α. Thus (7.1) is as in the theory of ideals; (7.2) is closer to $\mathfrak{A}$.

5. **The G.C.D., L.C.M. in $\mathfrak{L}$.** These afford interesting examples of invariance under formal equivalence. As first defined in $\mathfrak{A}$, the G.C.D. of a, b is the *greatest* integer which divides both a and b; the L.C.M. is the *least* integer which both a and b divide, division as always in $\mathfrak{A}$ being arithmetical, viz., all quotients are required to be in $\mathfrak{A}$. Neither of these is immediately applicable to $\mathfrak{L}$. But they may be replaced by their transforms in $\mathfrak{A}$, precisely as in the theory of ideals: *With every set of elements* $a, b, \cdots, h$ *of* $\mathfrak{A}$ *there is associated a unique element* m *of* $\mathfrak{A}$ *such that every element of* $\mathfrak{A}$ *which divides each element in the set divides also* m; *there also is associated a unique element* l *such that every element of* $\mathfrak{A}$ *which is a multiple of each element of the set is also a multiple of* l.

---

* If for $x \neq z'$ the relation xDy implies the existence in $\mathfrak{R}$ of a unique element w such that $y = xPw$, we say that the *quotient in* $\mathfrak{R}$ *is unique*

The propositions, if true, abstractly identical with these in any special ring $\mathfrak{R}'$ will be taken as the definitions of the *arithmetic G.C.D. and L.C.M. in* $\mathfrak{R}'$.

Abstracting these propositions to $\mathfrak{R}$, and taking D as in (6.1)–(6.3), we consider two operations G, L upon elements of $\mathfrak{R}$ such that, if x, y are any elements of $\mathfrak{R}$, then xGy and xLy are *uniquely* determined elements of $\mathfrak{R}$, and the postulates (8.1)–(9.4) are satisfied:

$$xGy = yGx, \tag{8.1}$$

$$xG(yGz) = (xGy)Gz \equiv xGyGz, \tag{8.2}$$

$$(xGy)Dx \,.\, (xGy)Dy, \tag{8.3}$$

$$zDx \,.\, zDy : \supset : zD(xGy), \tag{8.4}$$

for G; and for L,

$$xLy = yLx, \tag{9.1}$$

$$xL(yLz) = (xLy)Lz \equiv xLyLz, \tag{9.2}$$

$$xD(xLy) \,.\, yD(xLy), \tag{9.3}$$

$$xDz \,.\, yDz : \supset : (xLy)Dz, \tag{9.4}$$

in all of which x, y, z are any elements of $\mathfrak{R}$.

Note the abstract identity of the pairs (8.1), (9.1) and (8.2), (9.2) with $\mathfrak{R}_1$ and the first of $\mathfrak{R}_2$ in § 1, and observe the interesting reciprocal symmetry between (8.3), (8.4) and (9.3), (9.4).

A solution in $\mathfrak{A}$ of (8.1)–(9.4) is evidently $aGb \equiv$ the G.C.D. of the integers a, $b \geqq 0$, and of (9.1)–(9.4), $aLb \equiv$ the L.C.M. of a, b. Moreover (8.1)–(9.4) together with the postulated unicity of G, L define, or *uniquely determine*, the *arithmetic* G.C.D., L.C.M. of elements of $\mathfrak{A}$. Hence we shall call the solution in $\mathfrak{L}$ of (8.1)–(9.4) the *arithmetic G.C.D. and L.C.M. in* $\mathfrak{L}$, and by taking these properties of the G.C.D. and L.C.M. of *classes* as fundamental, we automatically fix *division and integral elements in* $\mathfrak{L}$.

There are two solutions, according to the choice of D as in either of (7.1), (7.2). The unicity, essential for arithmetic, is obvious in each instance. To indicate that we have now passed from algebra to arithmetic we shall use d, l, g as stated in § 1, instead of D, L, G, and write the definitions

$$\alpha d \beta \equiv \alpha \textit{ divides } \beta, \tag{10.1}$$

$$\alpha l \beta \equiv \textit{the L. C. M. of } \alpha, \beta \tag{10.2}$$

$$\alpha g \beta \equiv \textit{the G. C. D. of } \alpha, \beta, \tag{10.3}$$

$$(\zeta, \upsilon) \equiv \textit{the (zero, unity) in } \mathfrak{L}. \tag{10.4}$$

Assuming for the moment the existence and unicity of ζ, υ, we have the following alternative solutions of the problems of *arithmetic divisibility* (d), *greatest common divisor* (g), *least common multiple* (l) *in* $\mathfrak{L}$:

$$(11.1)\qquad \alpha d\beta \equiv \alpha \mid \beta, \qquad \alpha g\beta \equiv \alpha + \beta, \qquad \alpha l\beta \equiv \alpha\beta,$$

$$(11.2)\qquad \alpha d\beta \equiv \beta \mid \alpha, \qquad \alpha g\beta \equiv \alpha\beta, \qquad \alpha l\beta \equiv \alpha + \beta.$$

It will be of interest to write down the propositions which are the verifications of (8.1)–(9.4). The first column is for (11.1), the second for (11.2):

$$(8.11)\qquad \alpha + \beta = \beta + \alpha, \qquad \alpha\beta = \beta\alpha,$$

$$(8.21)\qquad \alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma, \qquad \alpha(\beta\gamma) = (\alpha\beta)\gamma,$$

$$(8.31)\qquad (\alpha + \beta) \mid \alpha \,.\, (\alpha + \beta) \mid \beta, \qquad \alpha \mid (\alpha\beta) \,.\, \beta \mid (\alpha\beta),$$

$$(8.41)\qquad \gamma \mid \alpha \,.\, \gamma \mid \beta : \supset : \gamma \mid (\alpha + \beta), \qquad \alpha \mid \gamma \,.\, \beta \mid \gamma : \supset : \alpha\beta \mid \gamma,$$

$$(9.11)\qquad \alpha\beta = \beta\alpha, \qquad \alpha + \beta = \beta + \alpha,$$

$$(9.21)\qquad \alpha(\beta\gamma) = (\alpha\beta)\gamma, \qquad \alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma,$$

$$(9.31)\qquad \alpha \mid (\alpha\beta) \,.\, \beta \mid (\alpha\beta), \qquad (\alpha + \beta) \mid \alpha \,.\, (\alpha + \beta) \mid \gamma,$$

$$(9.41)\qquad \alpha \mid \gamma \,.\, \beta \mid \gamma : \supset : \alpha\beta \mid \gamma, \qquad \gamma \mid \alpha \,.\, \gamma \mid \beta : \supset : \gamma \mid (\alpha + \beta).$$

6. **Addition (s) and multiplication (p) in $\mathfrak{L}$.** A fundamental property in $\mathfrak{A}$ of the G.C.D. and L.C.M. is that the *product* of the G.C.D. and L.C.M. of two elements of $\mathfrak{A}$ is equal to the *product* of the elements. This determines the choice of p and therefore also of s in $\mathfrak{L}$. As before there necessarily are two solutions. Each must (and does) satisfy $\mathfrak{R}_1$, $\mathfrak{R}_2$ of § 1. Writing

$$(12.1)\qquad \alpha s\beta \equiv \textit{the arithmetic sum of } \alpha,\beta,$$

$$(12.2)\qquad \alpha p\beta \equiv \textit{the arithmetic product of } \alpha,\beta,$$

we see that d, s, p must be paired as follows to preserve the property of g, l just mentioned:

$$(13.1)\qquad \alpha d\beta \equiv \alpha \mid \beta, \qquad \alpha s\beta \equiv \alpha + \beta, \qquad \alpha p\beta \equiv \alpha\beta\ ;$$

$$(13.2)\qquad \alpha d\beta \equiv \beta \mid \alpha, \qquad \alpha s\beta \equiv \alpha\beta, \qquad \alpha p\beta \equiv \alpha + \beta.$$

For *each* of the pairs (11.1), (13.1) and (11.2), (13.2) we have

$$(14)\qquad (\alpha g\beta)p(\alpha l\beta) = \alpha p\beta.$$

7. **The arithmetic zero ζ, unity υ, in $\mathfrak{L}$.** The algebraic zero, unity in $\mathfrak{L}$ are ω, ϵ, so that $\alpha+\omega=\alpha$, $\alpha\epsilon=\alpha$. In $\mathfrak{L}$ we must have

$$(15)\qquad \alpha s\zeta = \alpha, \qquad \alpha p\upsilon = \alpha,$$

for each element α of $\mathfrak{L}$. Hence in each of (13.1), (13.2), ζ, υ are uniquely determined, and we have

(15.1) $\quad \alpha s\beta \equiv \alpha + \beta, \quad \alpha p\beta \equiv \alpha\beta, \qquad (\zeta, \upsilon) = (\omega, \epsilon),$

(15.2) $\quad \alpha s\beta \equiv \alpha\beta, \qquad \alpha p\beta \equiv \alpha + \beta, \quad (\zeta, \upsilon) = (\epsilon, \omega).$

As in $\mathfrak{A}$ the unity in $\mathfrak{L}$ divides each element γ,

(16.1) $\quad \alpha d\beta \equiv \alpha \mid \beta, \quad \upsilon = \epsilon, \quad \upsilon d\gamma\ ;$

(16.2) $\quad \alpha d\beta \equiv \beta \mid \alpha, \quad \upsilon = \omega, \quad \upsilon d\gamma.$

Again, in $\mathfrak{A}$ the only element divisible by the zero in $\mathfrak{A}$ is zero, and in $\mathfrak{L}$ we have, in abstract identity* with $\mathfrak{A}$,

(17.1) $\quad \zeta \mid \gamma \,.\, (\gamma \neq \zeta) \,.\, (\zeta = \omega)$ is $(-)$,

(17.2) $\quad \gamma \mid \zeta \,.\, (\gamma \neq \zeta) \,.\, (\zeta = \epsilon)$ is $(-)$.

8. **Arithmetic congruence in $\mathfrak{L}$.** The proposition in $\mathfrak{L}$ abstractly identical with (1.5) in $\mathfrak{A}$ is

(18) $\quad (\alpha \equiv \zeta \bmod \mu) : \supset : \mu d\alpha,$

which is $(+)$ provided (cf. (4.1), (4.2) and (16.1), (16.2)) we pair as follows the definitions of congruence and divisibility in $\mathfrak{L}$:

(18.1) $\quad \alpha d\beta \equiv \alpha \mid \beta, \qquad (\alpha \equiv \beta \bmod \mu) \equiv \mu \mid (\alpha + \beta),$

(18.2) $\quad \alpha d\beta \equiv \beta \mid \alpha, \qquad (\alpha \equiv \beta \bmod \mu) \equiv \alpha\beta \mid \mu,$

which can be stated together as

(19) $\quad (\alpha \equiv \beta \bmod \mu) \equiv \mu d(\alpha s\beta) \equiv \mu d(\alpha g\beta).$

Since (18) is $(+)$ for each of (18.1), (18.2) it follows that the later are *necessary for arithmetic congruence c in $\mathfrak{L}$*. We have already satisfied (1.7) for c; it remains only to discuss (1.6).

9. **Residuals, completion of c, extremes.** The transformation by formal equivalence of (1.6) in $\mathfrak{A}$ will complete the sequence of properties of arithmetic congruence c in $\mathfrak{L}$ and yield the abstract identity of congruence in $\mathfrak{A}$, $\mathfrak{L}$. The necessary transformation, suggested by the properties of modular systems, is effected by the abstraction of Lasker's† concept of the residual for such systems. We shall first abstract to $\mathfrak{R}$.

---

* For $\omega \mid \omega$ cf. *Principia Mathematica*, 1st edition, p. 232, *24.13.

† Mathematische Annalen, vol. 60 (1905), p. 49.

Let a, b, l, m for the moment denote elements of $\mathfrak{R}$. Then, if m is uniquely determined by ($u' \equiv$ the unity in $\mathfrak{R}$),

$$\{aD(lPb)\} \,.\, \{mDl\} \,.\, \{m \neq u'\}, \tag{20}$$

where l runs through all elements in $\mathfrak{R}$, we shall call m the *residual of b with respect to a*, and we shall write $m = bRa$.

In $\mathfrak{L}$, (20) becomes

$$\{\alpha d(\lambda p \beta)\} \,.\, \{\mu d \lambda\} \,.\, \{\mu \neq \upsilon\} : \equiv : \mu \equiv \beta r \alpha\,, \tag{20.1}$$

where r replaces R in the instance (20.1) of (20), and λ is an arbitrary class.

In $\mathfrak{A}$, the residual of k with respect to m is the quotient of m by the G.C.D. of k and m, viz., this residual is m' in (1.6).

The proposition in $\mathfrak{L}$ abstractly identical with (1.6) is therefore

$$(\kappa p \alpha \equiv \kappa p \beta \bmod \mu) \supset (\alpha \equiv \bmod \kappa r \mu), \tag{21}$$

and this, as may be verified immediately, is implied by (20.1) and p, d, υ as in either of the following columns, which recapitulate previous solutions:

(s)	*Sum*:	$\alpha + \beta$,	$\alpha\beta$,	$\equiv \alpha s \beta$,
(p)	*Product*:	$\alpha\beta$,	$\alpha + \beta$,	$\equiv \alpha p \beta$,
(g)	*G.C.D. of* α, β:	$\alpha + \beta$,	$\alpha\beta$,	$\equiv \alpha g \beta$,
(l)	*L.C.M. of* α, β:	$\alpha\beta$,	$\alpha + \beta$,	$\equiv \alpha l \beta$,
(c)	$\alpha \equiv \beta \bmod \mu$:	$\mu \mid (\alpha + \beta)$,	$\alpha\beta \mid \mu$,	
(ζ)	*Zero*:	ω ,	ϵ ,	$\equiv \zeta$,
(υ)	*Unity*:	ϵ ,	ω ,	$\equiv \upsilon$,
(d)	α *divides* β:	$\alpha \mid \beta$,	$\beta \mid \alpha$,	$\equiv \alpha d \beta$,

the same interpretations for p, d, υ necessarily being taken in both of (20.1), (21).

Either column is implied by the other and the reciprocity between logical addition and multiplication. That $\alpha s \beta = \alpha g \beta$, $\alpha p \beta = \alpha l \beta$ in $\mathfrak{L}$, while the corresponding propositions in $\mathfrak{A}$ are (−), is due to the laws of tautology and absorption, but these do not destroy the abstract identity of the arithmetic of logic and rational arithmetic. The identity is in the fundamental propositions, or postulates, stated abstractly as in $\mathfrak{R}$, from which $\mathfrak{A}$ is developed, and we have shown therefore that certain parts of both rational arithmetic and the arithmetic of logic are instances of one and the same *content*. The abstract identity will be enhanced when we find a unique factorization law in $\mathfrak{L}$.

In passing it may be of interest to note the equivalents in $\mathfrak{L}$ of *least, greatest* in those parts of $\mathfrak{A}$ which we have abstracted. They are as follows. If in a given set of elements of $\mathfrak{L}$ there be a unique element different from the unity in $\mathfrak{L}$ which divides each element of the set, that element is called the *lower extreme* of the set; if in a given set of elements of $\mathfrak{L}$ there be a unique element different from the zero in $\mathfrak{L}$ which is divisible by each element of the set, that element is called the *upper extreme* of the set. In these definitions either type of division in $\mathfrak{L}$ may be taken; the upper and lower extremes, viz., the classes which these actually are, in either interpretation are inverted in the other. The G.C.D., L.C.M., residual and congruences in $\mathfrak{L}$ can be restated if desired in terms of extremes. If this be done the verbal forms in $\mathfrak{L}$ become the same as those in $\mathfrak{A}$.

10. **Unique factorization in $\mathfrak{L}$.** In $\mathfrak{A}$ a set of elements (integers $\geqq 0$) is said to be coprime if the G.C.D. of all members of the set is unity. Similarly in $\mathfrak{L}$ we define a set of elements to be *coprime* if their G.C.D. is v. In what follows it is assumed that we are operating in either one of the solutions for $s, p, g, l, c, \zeta, v, d$ exhibited in § 9; the results hold in either.

For clearness let us recall a few properties of the constituents ($\equiv$terms) of a Boole *development* ($\equiv$expansion*) which will be needed immediately. It is assumed that the development is in *normal form*, viz., that in which all terms with zero coefficients have been deleted. Then first, the logical product of any two distinct terms of a development is the logical zero. Otherwise stated, the terms of a Boole development are a set of classes such that any pair of them are mutually exclusive. The logical sum of all the terms is the logical unity. Hence if α, β denote any two identical (in which case $\beta \equiv \alpha$) or distinct terms of a development, $\alpha \mid \beta \supset \alpha = \beta$. Second, from a given set of classes we can generate by the operations of logical addition, multiplication and taking of supplements a set closed under these operations; the closed set consists of all the elements of $\mathfrak{L}$. The development of the logical unity of this set provides us with a set of terms such that the development of any element of $\mathfrak{L}$ as a function ($\equiv$logical sum) of such terms is unique. This situation is abstractly identical with the unique factorization theorem in $\mathfrak{A}$, as will be shown in a moment.

Suppose now that we have obtained the unique development as above described of a given element of $\mathfrak{L}$. Since $\mathfrak{L}$ is closed under the operation of taking the supplement, it follows that the development of any element of $\mathfrak{L}$ has a dual, obtained by taking the supplements of both sides of the original

---

* *Laws of Thought*, Chapter V, especially Prop. III.

development of the supplement of the given element. This gives us the dual unique decomposition in $\mathfrak{L}$ abstractly identical with the first and with the fundamental theorem of arithmetic.

In translating these properties of $\mathfrak{L}$ to arithmetic it is more intuitive to fix the attention on the second column in § 9. That is, we shall think of

$$\alpha s\beta \equiv \alpha\beta, \qquad \alpha p\beta \equiv \alpha + \beta, \qquad \alpha g\beta \equiv \alpha\beta, \qquad \alpha l\beta \equiv \alpha + \beta,$$

$$\zeta \equiv \epsilon, \qquad \upsilon \equiv \omega, \qquad \alpha d\beta \equiv \beta \mid \alpha,$$

although, by the duality in $\mathfrak{L}$, the theorems are valid in either interpretation. Arranging a few of the abstractly identical theorems and definitions of $\mathfrak{A}$, $\mathfrak{L}$ in pairs, we have the following:

(22.1) If the G.C.D. of a, b is 1, then a, b are called coprime.

(22.2) If the G.C.D. of α, β is υ, then α, β are called coprime.

(23.1) If k divides the product of a and b, and k, a are coprime, then k divides b.

(23.2) $\{\kappa d(\alpha p\beta)\}.(\kappa g\alpha = \upsilon) : \supset : \kappa d\beta.$

(24.1) q is prime if $k \neq 1$ divides q when and only when $k = q$.

(24.2) π is prime if and only if $(\kappa d\pi).(\kappa \neq \upsilon) : \supset : \kappa = \pi.$

(25.1) Primes exist; they are found by the seive of Eratosthenes and are a coprime set.

(25.2) Primes exist; they are found by the Boole development of ζ and are a coprime set.

(26.1) A positive integer is the product of primes in one way only.

(26.2) A given element of $\mathfrak{L}$ is the arithmetic product (p) of prime elements of $\mathfrak{L}$ in one way only.

This list can obviously be extended; for example we can write down the G.C.D. and L.C.M. of α, β from their resolutions into prime factors in $\mathfrak{L}$ precisely as in $\mathfrak{A}$. Again, abstractly identical with the theory of arithmetical functions in $\mathfrak{A}$, such as the indicator, sum and number of divisors, etc., of an integer, which depend upon the unique factorization law in $\mathfrak{A}$, there is a like theory of functions of classes or relations in $\mathfrak{L}$. Subtraction in this theory is as defined in $\mathfrak{L}$ by Boole. The interpretation in $\mathfrak{L}$ of these arithmetical theorems is however not always an easy matter; its interest here is that arithmetic has reacted upon logic to yield new results in the latter.

If to obtain the elements of $\mathfrak{L}$ we start from a finite set of classes (or relations) we have in the above arithmetic of $\mathfrak{L}$ a finite image of $\mathfrak{A}$. Conversely the theory of inclusion relations in logic is abstractly identical with rational arithmetic.

CALIFORNIA INSTITUTE OF TECHNOLOGY,
PASADENA, CALIF.