ABSTRACT RESIDUATION OVER LATTICES*

R. P. DILWORTH

Introduction. The idea of residuation goes back to Dedekind [3],† who introduced it in the theory of modules. It has since had extensive applications in the theory of algebraic modular systems [6], in the theory of ideals [8], and in certain topics of arithmetic [9]. On account of its fundamental role in several fields of modern algebra, it is desirable to consider residuation abstractly. A postulational treatment also is a necessary preliminary to the investigation of the structure properties of the residual. We give such an abstract formulation.

In a commutative ring with unit element the residual of an ideal B with respect to an ideal A, written $A:B$, is an ideal with the properties $A \supset (A:B)B$; if $A \supset XB$, then $A:B \supset X$. Although the residual is defined in terms of multiplication, most of its important properties are concerned with the cross-cut and union of ideals. Hence we shall consider a residual defined over a system having only these two operations, that is, over a *lattice* [2]. As an example of a system having a residual but no ordinary multiplication we consider in §5 residuation in a Boolean algebra.

In §1 the postulates for abstract residuation are given. Equality is taken as an undefined relation with cross-cut, union, and residual as undefined connections. In §2 we list a few systems satisfying the postulates. In §3 it is shown that the system defined by the postulates is a lattice and that the residual has all of its important properties which are independent of multiplication. Consistency and independence proofs are given in §4.

I wish to express my thanks to Professors Morgan Ward and E. T. Bell for their many suggestions and helpful criticisms during the preparation of this paper.

1. **Postulates for residuation.** Let Σ be a set of elements A, B, C, $\cdots$; and let $=$, $[\,,\,]$, $(\,,\,)$, and $:$ be relations, satisfying the postulates i–iv; 1–3; I–V. In what follows, $\circ$ denotes an arbitrary one of the relations $[\,,\,]$, $(\,,\,)$, $:$ and the letters A, B, C, $\cdots$, appearing in the statement of the postulates indicate arbitrary elements of Σ.

POSTULATE i. *$A \circ B$ is in Σ whenever A and B are in Σ.*

---

* Presented to the Society, November 27, 1937.

† Numbers in square brackets refer to the bibliography at the end of the paper.

POSTULATE ii. *If* $A=B$, *then* $C \circ A = C \circ B$ *and* $A \circ C = B \circ C$.*

POSTULATE iii. *If* $A=B$ *and* $B=C$, *then* $A=C$.

POSTULATE iv. *If* $A=B$, *then* $B=A$.

POSTULATE 1. $[[A, B], C] = [B, [A, C]]$.†

POSTULATE 2. $[A, A] = A$.

POSTULATE 3. *There is an element* I *in* Σ *such that* $[A, I] = A$ *for all* A *in* Σ.

As immediate deductions from these postulates we have:

1.1. $[I, A] = [A, I] = A$.

PROOF. $[I, A] = [I, [A, I]] = [[A, I], I] = [A, I] = A$ by ii, 1, 3, iii.

1.2. *The element* I *in Postulate* 3 *is unique.*

POSTULATE I. $A:A = I$.

POSTULATE II. $(A:B):C = (A:C):B$.

POSTULATE III. $A:(B, C) = [A:B, A:C]$.

POSTULATE IV. $[A, B]:C = [A:C, B:C]$.

POSTULATE V. *If* $A:B = B:A = I$, *then* $A = B$.

DEFINITION 1. $A:B = I$ is written $A \supset B$.

DEFINITION 2. $[A, B] = B$ is written $A > B$.

2. **Examples.** We list a few systems satisfying the postulates i–V.

1. Let Σ be the set of ideals in a commutative ring with unit element. Let $[\ ,\ ]$ and $(\ ,\ )$ be the cross-cut and union respectively. Let $A:B$ be defined by $A \supset (A:B)B$, if $A \supset XB$, $A:B \supset X$.

2. Let Σ be the set of positive integers with $[\ ,\ ]$ and $(\ ,\ )$ the L. C. M. and G. C. D. respectively. Let $A:B$ be defined by $A/(A, B)$ with $I=1$.

3. As in 2, let Σ be the set of positive integers with $[\ ,\ ]$ and $(\ ,\ )$ defined as max $(\ ,\ )$ and min $(\ ,\ )$ respectively. If now $A:B$ is defined by max $(0, A-B)$ and 0 is taken to be the element I, the postulates are satisfied.

4. Let Σ be the integers $\leqq n$ with $[\ ,\ ]$ and $(\ ,\ )$ defined by min $(\ ,\ )$ and max $(\ ,\ )$, respectively. Define $A:B$ as min $(n, n+A-B)$ with $I=n$.

5. Let Σ be a Boolean algebra with $[\ ,\ ]$, $(\ ,\ )$ the Boolean operations $\cdot$, $\vee$ respectively. Let $A:B = A \vee B'$.

* It is understood that the relations in the postulates hold whenever the respective elements and the indicated combinations are in Σ.

† To facilitate obtaining an independence example, the commutative and associative laws have been combined in one postulate.

3. **Deductions from the postulates.** † We have, first,

2.1. $A = A$ by 3, iv.

2.12. *$A \supset B$ and $B \supset A$ is equivalent to $A = B$* ‡ by V, Definition 1.

2.13. *If $M:A = M:B$ for all M in Σ, then $A = B$.*

PROOF. $M = A$, B respectively give

2.14. $A:B = A:A = I$ and $B:A = B:B = I$ by ii, I, iv.

Hence $A = B$ by V.

2.15. $[A, B] = [B, A]$.

PROOF. $[A, B] = [[A, B], I] = [B, [A, I]] = [B, A]$ by 3, 1, 3, ii.

2.16. $(A, B) = (B, A)$ by III, 2.15, 2.13.

2.17. $[[A, B], C] = [A, [B, C]]$ by 2.15, 1.

2.18. $((A, B), C) = (A, (B, C))$ by III, 2.17, III, 2.13.

From 2.17 and 2.18 we may write $[A, B, C]$ for $[[A, B], C]$ and (A, B, C) for $((A, B), C)$. Generally $[A_1, A_2, \cdots, A_n]$, $(A_1, A_2, \cdots, A_n)$ are unambiguous.

*2.19. $M:(A_1, A_2, \cdots, A_n) = [M:A_1, M:A_2, \cdots, M:A_n]$ by induction from III.

*2.2. $[A_1, A_2, \cdots, A_n]:M = [A_1:M, A_2:M, \cdots, A_n:M]$ by induction from IV.

2.22. $(A, A) = A$.

PROOF. $M:(A, A) = [M:A, M:A] = [M, M]:A = M:A$ by III, IV, 2. Hence $(A, A) = A$ by 2.13.

2.23. $(A, B) \supset A$.

PROOF. $(A, B):A = [(A, B):A, I] = [(A, B):A, (A, B):(A, B)] = (A, B):(A, (A, B)) = (A, B):((A, A), B) = (A, B):(A, B) = I$ by 3, I, III, 2.18, 2.22, I.

2.24. *If $A > B$, then $A \supset B$.*

PROOF. $[A, B] = B$ gives $A:B = [A:B, I] = [A:B, B:B] = [A, B]:B = B:B = I$ by 3, I, IV, I.

2.25. *If $[A, B] = B$, then $(A, B) = A$.*

PROOF. $A:(A, B) = [A:A, A:B] = [I, A:B] = A:B = I$ by III, I, 3, 2.24. Hence $(A, B) = A$ by 2.23, V.

2.26. $(A, I) = (I, A) = I$ by 2.25, 3, 2.16.

† The theorems giving the essential properties of the residual will be starred.

‡ By "equivalent" we mean formal equivalence.

*2.27. $I:A=I$.

PROOF. $I:A=[I,\ I:A]=[I:I,\ I:A]=I:(I,\ A)=I:I=I$ by 1.1, I, III, 2.26, I.

*2.28. $A:I=A$.

PROOF. $(A:(A:I)):I=(A:I):(A:I)=I$ by II, I. $I:(A:(A:I))=I$ by 2.27. Hence $A:(A:I)=I$ by V. But $(A:I):A=(A:A):I=I:I=I$ by II, I. Hence $A:I=A$ by V.

2.29. $A \supset [A, B]$ by 2.17, 2, 2.24.

2.3. *If* $A \supset B$, *then* $A > B$.

PROOF. $[A,\ B]:B=[A:B,\ B:B]=[I,\ I]=I$ by IV, I, 2. But $B:[A,\ B]=I$ by 2.29, 2.15, Definition 1. Hence $[A,\ B]=B$ by V.

2.31. $A \supset B$ *is equivalent to* $A > B$ by 2.24, 2.3.

2.32. $(A,\ [A,\ B])=A$ by 2.29, 2.31, 2.25.

2.33. $[A,\ (A,\ B)]=A$ by 2.23, 2.31, Definition 2.

2.34. Σ *is a lattice.*

PROOF. We show that Birkhoff's axioms L1–L4† are satisfied if we take $[\ ,\ ] \equiv \cap$. For L1 is i; L2 is 2.15 and 2.16; L3 is 2.17 and 2.18; L4 is 2.32 and 2.33.

*2.35. $A:(A:B) \supset B$ by II, I.

*2.4. *If* $B \supset C$, *then* $A:C \supset A:B$.

PROOF. $A:(A:B) \supset B$ and $B \supset C$ by 2.35. Hence $(A:(A:B)):C = I$ by 2.34, Definition 1. Then $(A:C):(A:B) = (A:(A:B)):C = I$ by II.

*2.41. $A:B=A:(A,\ B)$ by III, I, 1.1.

*2.42. $[A,\ B]:B=A:B$ by II, I, 3.

*2.43. $I \supset A:B \supset A$ by 2.27, II, I, 2.27.

*2.44. $A:(A:(A:B))=A:B$.

PROOF. $[A:(A:(A:B))]:(A:B)=[A:(A:B)]:[A:(A:B)]=I$ by II, I. $(A:B):[A:(A:(A:B))]=[A:[A:(A:(A:B))]]:B=I$ by II. Since $A:[A:(A:(A:B))] \supset A:(A:B)$ and $A:(A:B) \supset B$ by 2.35, hence $A:(A:(A:B))=A:B$ by V.

It will be noted from 2.44 that $A:(A:B)$ and $A:B$ are mutually residual with respect to A.

*2.45. *If* $A:C=A:B$, *then* $A:(A:B) \supset C$ by II, I.

---

† G. Birkhoff, *On the lattice theory of ideals*, this Bulletin, vol. 40 (1934), p. 613. L1, L2, L3, and L4 are his axioms for a lattice.

These theorems are sufficient to show that the usual properties of the residual are deducible from the postulates of §1.

Since the residual as here considered is independent of multiplication, there is a residual completely dual to that defined above. The dual may be defined by the postulates I′–V′:

POSTULATE I′. *$A:A=E$ where E is the null element of the lattice.*
POSTULATE II′. $(A:B):C=(A:C):B$.
POSTULATE III′. $A:[B, C]=(A:B, A:C)$.
POSTULATE IV′. $(A, B):C=(A:C, B:C)$.
POSTULATE V′. *If $A:B=B:A=E$, then $A=B$.*

Thus, for the integers 0, 1, 2, $\cdots$, n as the given set, let [,], (,) be defined as min (,), max (,) respectively with $E=0$ and $I=n$. Then $A:B\equiv\min(n, n+A-B)$ is a residual satisfying the postulates of §1, while $A:B\equiv\max(0, A-B)$ is a residual satisfying the second set of postulates.

4. Consistency and independence proofs. †

	[,]	(,)	:	
Consistency	$\begin{array}{c\|cc} & 1 & 2 \\ \hline 1 & 1 & 2 \\ 2 & 2 & 2 \end{array}$	$\begin{array}{c\|cc} & 1 & 2 \\ \hline 1 & 1 & 1 \\ 2 & 1 & 2 \end{array}$	$\begin{array}{c\|cc} & 1 & 2 \\ \hline 1 & 1 & 1 \\ 2 & 2 & 1 \end{array}$	
Independence				
1	$\begin{array}{c\|ccc} & 1 & 2 & 3 \\ \hline 1 & 1 & 1 & 2 \\ 2 & 2 & 2 & 2 \\ 3 & 3 & 3 & 3 \end{array}$	$\begin{array}{c\|ccc} & 1 & 2 & 3 \\ \hline 1 & 1 & 1 & 1 \\ 2 & 2 & 2 & 2 \\ 3 & 2 & 3 & 3 \end{array}$	$\begin{array}{c\|ccc} & 1 & 2 & 3 \\ \hline 1 & 1 & 1 & 1 \\ 2 & 2 & 1 & 1 \\ 3 & 3 & 2 & 1 \end{array}$	$[[1, 3], 2]\neq[3, [1, 2]]$
2	$\begin{array}{c\|cc} & 1 & 2 \\ \hline 1 & 1 & 2 \\ 2 & 2 & 1 \end{array}$	$\begin{array}{c\|cc} & 1 & 2 \\ \hline 1 & 2 & 1 \\ 2 & 1 & 2 \end{array}$	$\begin{array}{c\|cc} & 1 & 2 \\ \hline 1 & 1 & 1 \\ 2 & 2 & 1 \end{array}$	$[2, 2]\neq 2$
3	$\begin{array}{c\|ccc} & 1 & 2 & 3 \\ \hline 1 & 1 & 1 & 1 \\ 2 & 1 & 2 & 1 \\ 3 & 1 & 1 & 3 \end{array}$	$\begin{array}{c\|ccc} & 1 & 2 & 3 \\ \hline 1 & 1 & 3 & 3 \\ 2 & 3 & 2 & 3 \\ 3 & 3 & 3 & 3 \end{array}$	$\begin{array}{c\|ccc} & 1 & 2 & 3 \\ \hline 1 & 1 & 1 & 1 \\ 2 & 2 & 1 & 1 \\ 3 & 3 & 2 & 1 \end{array}$	$[2, 1]\neq 2, [3, 2]\neq 3, [2, 3]\neq 2$
I	$\begin{array}{c\|cc} & 1 & 2 \\ \hline 1 & 1 & 2 \\ 2 & 2 & 2 \end{array}$	$\begin{array}{c\|cc} & 1 & 2 \\ \hline 1 & 1 & 1 \\ 2 & 1 & 2 \end{array}$	$\begin{array}{c\|cc} & 1 & 2 \\ \hline 1 & 1 & 1 \\ 2 & 2 & 2 \end{array}$	$2:2\neq 1$

	[,]	(,)	:	
II	$\begin{array}{c\|ccc} & 1 & 2 & 3 \\ \hline 1 & 1 & 2 & 3 \\ 2 & 2 & 2 & 3 \\ 3 & 3 & 3 & 3 \end{array}$	$\begin{array}{c\|ccc} & 1 & 2 & 3 \\ \hline 1 & 1 & 1 & 1 \\ 2 & 1 & 2 & 2 \\ 3 & 1 & 2 & 3 \end{array}$	$\begin{array}{c\|ccc} & 1 & 2 & 3 \\ \hline 1 & 1 & 1 & 1 \\ 2 & 3 & 1 & 1 \\ 3 & 3 & 2 & 1 \end{array}$	$(3:1):2 \neq (3:2):1$
III	$\begin{array}{c\|cc} & 1 & 2 \\ \hline 1 & 1 & 2 \\ 2 & 2 & 2 \end{array}$	$\begin{array}{c\|cc} & 1 & 2 \\ \hline 1 & 1 & 1 \\ 2 & 2 & 2 \end{array}$	$\begin{array}{c\|cc} & 1 & 2 \\ \hline 1 & 1 & 1 \\ 2 & 2 & 1 \end{array}$	$2:(2, 1) \neq [2:2, 2:1]$
IV	$\begin{array}{c\|cccc} & 1 & 2 & 3 & 4 \\ \hline 1 & 1 & 2 & 3 & 4 \\ 2 & 2 & 2 & 3 & 4 \\ 3 & 3 & 3 & 3 & 4 \\ 4 & 4 & 4 & 4 & 4 \end{array}$	$\begin{array}{c\|cccc} & 1 & 2 & 3 & 4 \\ \hline 1 & 1 & 1 & 1 & 1 \\ 2 & 1 & 2 & 2 & 2 \\ 3 & 1 & 2 & 3 & 3 \\ 4 & 1 & 2 & 3 & 4 \end{array}$	$\begin{array}{c\|cccc} & 1 & 2 & 3 & 4 \\ \hline 1 & 1 & 1 & 1 & 1 \\ 2 & 2 & 1 & 1 & 1 \\ 3 & 3 & 3 & 1 & 1 \\ 4 & 4 & 2 & 2 & 1 \end{array}$	$[4, 3]:2 \neq [4:2, 3:2]$
V	$\begin{array}{c\|cc} & 1 & 2 \\ \hline 1 & 1 & 2 \\ 2 & 2 & 2 \end{array}$	$\begin{array}{c\|cc} & 1 & 2 \\ \hline 1 & 1 & 1 \\ 2 & 1 & 2 \end{array}$	$\begin{array}{c\|cc} & 1 & 2 \\ \hline 1 & 1 & 1 \\ 2 & 1 & 1 \end{array}$	$2:1 = 1:2 = 1$ but $2 \neq 1$.

† The independence examples for i–iv are omitted.

5. **Residuation in a Boolean algebra** [1]. If we take Σ to be a Boolean algebra and interpret [,], (,) as the Boolean operations $\cdot$, $\vee$ respectively, then it is readily verified that Σ satisfies postulates i–V if we define residuation by $A:B \equiv A \vee B'$. Moreover we have the following theorem:

THEOREM. *Let Σ be a Boolean algebra and let* [,], (,) *be the Boolean operations* $\cdot$, $\vee$ *respectively. Then the only Boolean operation satisfying postulates* I–V *is* $A:B = A \vee B'$.

PROOF. Write $A:B$ as a general Boolean function of A and B

$$A:B = K_1AB \vee K_2AB' \vee K_3A'B \vee K_4A'B'.$$

Then

$$1:1 = K_1 = 1, \qquad 0:1 = K_3 = 0,$$

$$1:0 = K_2 = 1, \qquad 0:0 = K_4 = 1.$$

Hence

$$A:B = AB \vee AB' \vee A'B' = A(B \vee B') \vee A'B' = A \vee A'B'$$

$$= (A \vee AB') \vee A'B' = A \vee (A \vee A')B' = A \vee B',$$

and as above this is sufficient that postulates I–V be satisfied.

With this definition of $A:B$, $A \supset B$ becomes the usual inclusion relation of the algebra of classes [5].

REFERENCES

1. E. T. Bell, *Arithmetic of logic*, Transactions of this Society, vol. 29 (1927), pp. 597–611.

2. Garrett Birkoff, *On combination of subalgebras*, Cambridge Philosophical Society Proceedings, vol. 29 (1933), pp. 441–464.

3. R. Dedekind, *Dirichlet, Vorlesungen über Zahlentheorie.*

4. E. Lasker, *Zur Theorie der Moduln und Ideale*, Mathematische Annalen, vol. 60 (1905), pp. 20–115.

5. Lewis and Langford, *Symbolic Logic*, 1932.

6. F. S. Macaulay, *The Algebraic Theory of Modular Systems*, Cambridge Tracts, no. 19, 1916.

7. O. Ore, *Abstract Algebra* I, II, Annals of Mathematics, vol. 36 (1935), pp. 406–437; vol. 37 (1936), pp. 265–292.

8. B. L. van der Waerden, *Moderne Algebra*, vol. 2.

9. M. Ward, *Some arithmetical applications of residuation*, American Journal of Mathematics, vol. 59 (1937), pp. 921–926.

CALIFORNIA INSTITUTE OF TECHNOLOGY

A NOTE ON THE MAXIMUM PRINCIPLE FOR ELLIPTIC DIFFERENTIAL EQUATIONS

FRITZ JOHN

Let $u(x_1, \cdots, x_n)$ denote a twice continuously differentiable function of $x_1, \cdots, x_n$ in some region R. We write $\partial u/\partial x_i = u_i$, $\partial^2 u/\partial x_i \partial x_k = u_{ik}$, and occasionally (x) for $(x_1, \cdots, x_n)$. A point $(c) = (c_1, \cdots, c_n)$ of R may be called a *proper* maximum of u, if

$$u_i(c) = 0 \qquad \text{for} \qquad i = 1, \cdots, n,$$

$$\sum_{i,k} u_{ik}(c)\xi_i\xi_k < 0 \qquad \text{for all} \qquad (\xi_1, \cdots, \xi_n) \neq (0, \cdots, 0).$$

A partial differential equation

$$\sum_{i,k} a_{ik}(x)u_{ik}(x) + \sum_i b_i(x)u_i(x) = 0 \tag{1}$$

(where the a_{ik} and b_i are defined in R) is called *elliptic* if for every (x) of R

$$\sum_{i,k} a_{ik}(x)\xi_i\xi_k \geqq 0$$

for all $(\xi_1, \cdots, \xi_n)$ and <0 for some $(\xi_1, \cdots, \xi_n)$.