SOME ARITHMETICAL APPLICATIONS OF RESIDUATION.

By Morgan Ward.

1°. The operation of residuation was apparently first considered by Dedekind in his theory of the modules in a ring of algebraic integers [1].[1] It was introduced into polynomial ideal theory by Emanuel Lasker [2], and has since been used systematically by F. S. Macaulay [3] and others. I propose to show here how the operation may be applied to various arithmetical problems,[2] in particular to developing a systematic calculus for the periods of elements in any finite Abelian group.

2°. Consider first for simplicity a cyclic group $\mathfrak{G}$ of order N written additively. Every element α of $\mathfrak{G}$ may be uniquely represented as

$$\alpha = a\gamma, \qquad 0 < a \leqq N \tag{2.1}$$

where γ is a fixed primitive element of $\mathfrak{G}$ and $a\gamma$ means $\gamma + \gamma + \cdots + \gamma$ taken a times. We write L_α for a in (2.1); for example $L_0 = N$. Let P_α denote the period of α; that is the least positive integer p such that $p\alpha = 0$. The starting point of our investigation is the observation that *P_α is the residual of L_α with respect to N.*

L_ξ considered as an operation on $\mathfrak{G}$ to the finite ring K_N of the integers modulo N is linear and distributive:

$$L_{m\alpha+n\beta} \equiv mL_\alpha + nL_\beta \pmod{N}, \qquad m,\ n \text{ integers.}$$

On the other hand, P_ξ is neither a linear nor a distributive operation; given P_α and P_β, all we can assert about $P_{\alpha+\beta}$ is that it divides $[P_\alpha, P_\beta]$, the least

[1] The numbers [1], [2], $\cdots$ in square brackets refer to the bibliography at the close of the paper.

[2] For example, consider the problem of solving

$$AX \equiv 0\ (\text{modd}\ \mathfrak{m}, F). \tag{1}$$

Here A and F are given polynomials in indeterminates $x_1, \cdots, x_s$ with coefficients in a commutative ring $\mathfrak{R}$ while $\mathfrak{m}$ is an ideal of $\mathfrak{R}$. We seek all solutions X in the quotient ring $\mathfrak{R}[x_1, \cdots, x_s]/\mathfrak{m}$. If $\mathfrak{A}$ and $\mathfrak{F}$ denote the ideals $(\mathfrak{m}, A)$, $(\mathfrak{m}, F)$ then the totality of such solutions of (1) constitute the residual ideal of $\mathfrak{A}$ with respect to $\mathfrak{F}$ (Van der Waerden [4] Chapter XII). Thus the solution of (1) is equivalent to specifying this residual, say by determining a basis for it. I have given a complete solution for the case when $s = 1$ and $\mathfrak{R}$ is the ring of rational integers. Ward [5].

common multiple of P_α and P_β.[3] Simple numerical examples show that $P_{\alpha+\beta}$ may be any divisor whatever of $[P_\alpha, P_\beta]$.

These facts suggest that we introduce in $\mathfrak{G}$ one or more new operations $\xi \circ \eta$, $\xi \times \eta$ such that $P_{\alpha\circ\beta}$, $P_{\alpha\times\beta}$ may be calculated knowing only the values of P_α, P_β; the definition of P_α as a residual immediately suggests how these operations should be defined. But before introducing these operations, we shall briefly summarize the properties of residuation of which we make use.

3. Let $\mathfrak{O}$ be the set of ideals[4] $A, B, C, \cdots$ of a fixed commutative ring containing a unit element. If A and B are any two elements of $\mathfrak{O}$, the residual of B with respect to A is by definition an ideal C such that

$$A \supset BC; \quad \text{if} \quad A \supset BX \quad \text{then} \quad C \supset X.$$

We write as usual $C = A:B$. The residual always exists and has the following properties:

$$\begin{aligned}
(3.1) \qquad & A:B = A:(A,B) = [A,B]:B, \\
& (A:B):C = (A:C):B = A:BC, \\
& A = M:N \text{ and } B = M:(M:N) \text{ imply } B = M:A,\ A = M:B, \\
& M:(A_1, A_2, \cdots, A_k) = [M:A_1, M:A_2, \cdots, M:A_k], \\
& [A_1, A_2, \cdots, A_k]:M = [A_1:M, A_2:M, \cdots, A_k:M].
\end{aligned}$$

If we restrict $\mathfrak{O}$ to be a principal ideal ring, then $A \supset B$ if and only if there exists a quotient $Q = A/B$ such that $A = QB$. Furthermore this quotient is unique. It is easily shown that $A:B = A/B$ whenever the quotient A/B exists, so that formula (3.1) becomes

$$(3.11) \qquad A:B = \frac{A}{(A,B)} = \frac{B}{[A,B]}.$$

On using this result and the unicity of the quotient, we easily find that the following additional rules for residuation hold in any principal ideal ring.[5]

$$\begin{aligned}
(M,N) = M:(M:N), \qquad & M:AB = \{(M:A)(M:B)\}:M, \\
(A_1, A_2, \cdots, A_k):M &= (A_1:M, \cdots, A_k:M), \\
M:[A_1, A_2, \cdots, A_k] &= (M:A_1, \cdots, M:A_k).
\end{aligned}$$

[3] We use $(A, B, \cdots)$, $[A, B, \cdots]$ both for the union and join of ideals $A, B, \cdots$ or the greatest common divisor and least common multiple of integers $A, B, \cdots$.

[4] We use the notation of van der Waerden [4], chapter XII save that roman capitals are used for ideals instead of gothic capitals.

[5] A detailed analysis of the properties of residuation, is given in Ward [6], Dilworth [7].

4°. The formulas of section **3°** give the fundamental relations

$$(4.\,1)\qquad P_a = N : L_a = \frac{N}{(N, L_a)} = \frac{[N, L_a]}{L_a}\,,$$

$$P_a = N : (N : P_a),\ L_a = N : P_a \text{ if and only if } L_a \text{ divides } N.$$

We define our new operations over the group $\mathfrak{G}$ as follows. We write

$$\delta = (\xi, \eta) \text{ if } L_\delta = (L_\xi, L_\eta),$$
$$\mu = [\xi, \eta] \text{ if } L_\mu \equiv [L_\xi, L_\eta] \pmod{N}.$$

It is clear that the group $\mathfrak{G}$ forms an arithmetic structure[6] with respect to the operations of union and cross-cut thus defined which is simply isomorphic with the structure of the ring K_N.

The third operation over $\mathfrak{G}$ which we shall consider is a multiplication simply isomorphic with multiplication in K_N: we write

$$\pi = \xi \cdot \eta \text{ if } L_\pi \equiv L_\xi L_\eta \pmod{N}.$$

If we call two elements of $\mathfrak{G}$ equivalent if and only if each divides the other, then equivalent elements have the same period and conversely.

The periods of δ, μ and π obey the following simple rules which are easy consequences of (4. 1) and the formulas of section **3°**:

$$P_{(\xi,\eta)} = [P_\xi, P_\eta], \quad P_{(\xi_1, \xi_2, \ldots, \xi_k)} = [P_{\xi_1}, P_{\xi_2}, \cdots, P_{\xi_k}],$$
$$P_{[\xi,\eta]} = (P_\xi, P_\eta), \quad P_{[\xi_1, \xi_2, \ldots, \xi_k]} = (P_{\xi_1}, P_{\xi_2}, \cdots, P_{\xi_k}),$$
$$P_{\xi\,.\,\eta} = \{P_\xi P_\eta\} : N, \ P_{\xi_1\,.\,\xi_2\,.\,\ldots\,.\,\xi_k} = \{P_{\xi_1} P_{\xi_2} \cdots P_{\xi_k}\} : N^{k-1}.$$

Thus for each operation the period is readily calculated from the period of its constituents. It is possible to define a residual $\xi : \eta$ in $\mathfrak{G}$ by $L_{\xi:\eta} = L_\xi : L_\eta$, but its period is not calculable in terms of the periods of ξ and η alone.

5°. If we choose a different primitive element γ' in place of γ defining a new operator L'_ξ over $\mathfrak{G}$ we have

$$L'_a \equiv L'_\gamma L_a \pmod{N}, \qquad L_a \equiv L_{\gamma'} L'_a \pmod{N}$$

where $L'_\gamma L_{\gamma'} \equiv 1 \pmod{N}$, so that both L'_γ and $L_{\gamma'}$ are prime to N. It readily follows that the operations (ξ, η), $[\xi, \eta]$ are independent of the particular base γ chosen to define them. The situation for the product is different. We

[6] Or distributive lattice. See Ore [8] or Ward [6] for detailed definition.

find that $(\alpha\cdot\beta)' = \gamma'\cdot(\alpha\cdot\beta)$. On the other hand $P'_a = P_a$. The formulas (4.1) are thus unchanged. For example:

$$P'_{(\xi\,.\,\eta)'} = P_{\gamma'\,.\,(\xi\,.\,\eta)} = \{P_{\gamma'} P_{\xi\,.\,\eta}\} : N = \{N\,.\,P_{\xi\eta}\} : N = P_{\xi\eta}.$$

6°. Suppose now that the group $\mathfrak{G}$ is the direct sum of κ cyclic groups $\mathfrak{G}^{(1)}, \cdots, \mathfrak{G}^{(k)}$ of orders $N^{(1)}, \cdots, N^{(k)}$:

$$\mathfrak{G} = \mathfrak{G}^{(1)} \dotplus \mathfrak{G}^{(2)} \dotplus \cdots \dotplus \mathfrak{G}^{(i)} \dotplus \cdots \dotplus \mathfrak{G}^{(k)}, \tag{6.1}$$

so that the typical element α of $\mathfrak{G}$ is of the form

$$\alpha = \alpha^{(1)} + \alpha^{(2)} + \cdots + \alpha^{(i)} + \cdots + \alpha^{(k)}.$$

We select in each group $\mathfrak{G}^{(i)}$ a primitive element $\gamma^{(i)}$ and define operators $L_a{}^{(i)}$ as in section **2°** by

$$L_a{}^{(i)} = a^{(i)}, \qquad \alpha^{(i)} = a^{(i)}\gamma^{(i)}, \qquad\qquad (i = 1, 2, \cdots, k).$$

We then associate with the element α the vector $\mathfrak{L}_a$ whose i-th component is $L_a{}^{(i)}$. The operations (α,β), $[\alpha,\beta]$ $\alpha\cdot\beta$ over $\mathfrak{G}$ of union, cross-cut and product are defined by the vectors $\mathfrak{L}_{(\alpha,\beta)}$, $\mathfrak{L}_{[\alpha,\beta]}$, $\mathfrak{L}_{\alpha\,.\,\beta}$ with components $(L_a{}^{(i)}, L_\beta{}^{(i)})$, $[L_a{}^{(i)}, L_\beta{}^{(i)}]$, $L_a{}^{(i)}L_\beta{}^{(i)}$ respectively where the components are taken modulo $N^{(i)}$ in the associated rings $K_{N^{(i)}}$.

With an obvious extension of notation, we write

$$\mathfrak{L}_{(\alpha,\beta)} = (\mathfrak{L}_\alpha, \mathfrak{L}_\beta), \qquad \mathfrak{L}_{[\alpha,\beta]} = [\mathfrak{L}_\alpha, \mathfrak{L}_\beta]$$
$$\mathfrak{L}_{\alpha\,.\,\beta} = \mathfrak{L}_\alpha \cdot \mathfrak{L}_\beta.$$

The *vectorial period* of α is defined as the vector $\mathfrak{P}_\alpha$ with components $P_a{}^{(i)} = N^{(i)} : L^{(i)}$. If $\mathfrak{N}$ denotes the vector with components $N^{(1)}, N^{(2)}, \cdots, N^{(k)}$ ($\mathfrak{N}$ is simply $\mathfrak{L}_0$, where 0 is the identity element of $\mathfrak{G}$) then we write

$$\mathfrak{P}_\alpha = \mathfrak{N} : \mathfrak{L}_\alpha.$$

These definitions allow us to extend immediately the formulas of section **4°**; thus

$$\mathfrak{P}_{[\alpha,\beta]} = (\mathfrak{P}_\alpha, \mathfrak{P}_\beta), \qquad \mathfrak{P}_{(\alpha,\beta)} = [\mathfrak{P}_\alpha, \mathfrak{P}_\beta], \qquad \mathfrak{P}_{\alpha\,.\,\beta} = \mathfrak{P}_\alpha \cdot \mathfrak{P}_\beta : \mathfrak{N}.$$

The actual period of α (that is, the least positive integer p such that $p\alpha = 0$) is simply the least common multiple of the components of the vectorial period. Denoting it as before by P_a, we have

$$P_a = [P_a{}^{(1)}, P_a{}^{(2)}, \cdots, P_a{}^{(k)}].$$

We cannot calculate the scalar period of $\alpha \cdot \beta$ or $[\alpha, \beta]$ directly in terms of the scalar periods of α and β. But for the union (α, β) we have the elegant formula

$$P_{(\alpha, \beta)} = [P_\alpha, P_\beta].$$

These considerations apply to any finite Abelian group since every such group may be represented as a direct sum of cyclic groups. If we assume as is always possible that the order of each summand is a power of a prime, then the number of summands $\mathfrak{G}^{(i)}$ is uniquely specified and also the orders ${}^{N^{(i)}}$.

To remove in part the ambiguity in the definition of the components of $\mathfrak{L}_\xi$ and $\mathfrak{P}_\xi$ due to the fact that the order of the groups $\mathfrak{G}^{(i)}$ in (6.1) is unspecified, we agree to arrange the prime power orders $N^{(i)}$ first in the natural order of the primes, and then arrange the powers of each prime in order of magnitude. The remaining ambiguity in the order of the components due to adjoining isomorphic groups in the decomposition (6.1) appears to be inherent, as the set of all vector functions $\mathfrak{P}_\xi$ over $\mathfrak{G}$ can be regarded as a basis for a representation of the group of automorphisms of $\mathfrak{G}$, each function being corollated with the sub-group of automorphisms leaving its components unchanged in order, but changing possibly the basis elements $\gamma^{(i)}$ in terms of which the components $L_\xi{}^{(i)}$ are specified. We have already seen in section **5**° that the components of $\mathfrak{P}_\xi$ are unaffected by such changes of base. The remaining automorphisms of $\mathfrak{G}$ will permute isomorphic groups in (6.1) thus inducing a permutation of the vector functions $\mathfrak{P}_\xi$. In any event the scalar period function P_ξ remains unaffected.

Since any finite field excluding its zero element is a cyclic group with respect to multiplication, the calculus we have developed in section **4**° carries over entire to the periods of elements in any such field. The vectorial calculus of the present section similarly applies to the periods of the units in any finite commutative ring.

7°. The operations which we have defined over the finite group have analogues in common arithmetic. For if

$$A = \prod_1^\infty P_n{}^{a_n}, \qquad B = \prod_1^\infty P_n{}^{b_n}$$

are the decompositions of the positive integers A and B into their prime factors, where $P_1, P_2, P_3, \cdots$ denote the primes $2, 3, 5, \cdots$ in their natural order and only a finite number of the exponents a_n, b_n are not zero, we may define a "union," "cross-cut" and "product" of A and B "of the second kind" by

$$(A, B) = \prod_1^\infty P_n{}^{(a_n, b_n)} \qquad [A, B] = \prod_1^\infty P_n{}^{[a_n, b_n]}$$

$$A \cdot B = \prod_1^\infty P_n{}^{a_n, b_n}.$$

The product of the second kind is distributive with respect to the ordinary product $A \times B$ or " product of the first kind ":

$$A \cdot (B \times C) = (A \cdot B) \times (A \cdot C).$$

The analogy with our treatment of groups becomes evident if we think of A as specified by the vector with components $a_1, a_2, \cdots$.

Indeed our product is the arithmetical analogue of the " multiplication of the second order " considered by De Morgan [9] and others [10] in the hierarchy of operations

$$A + B,\ A \times B = \exp(\log A + \log B),\ A \cdot B = \exp(e^{\log\log A + \log\log B}) = A^{\log B}, \cdots.$$

Pasadena, California.

REFERENCES.

1. R. Dedekind, Supplement XI of Dirichlet's *Vorlesungen*, 4th edition (1894), § 170; *Collected Works*, vol. III, p. 71.
2. E. Lasker, *Mathematische Annalen*, vol. 60 (1905), pp. 20-116.
3. F. S. Macaulay, *The Algebraic Theory of Modular Systems*, Cambridge (1916).
4. B. L. van der Waerden, *Moderne Algebra*, vol. 2 (Berlin, 1931).
5. M. Ward, *Transactions of the American Mathematical Society*, vol. 35 (1933), pp. 254-260.
6. M. Ward, Paper submitted to the *Duke Journal*.
7. R. P. Dilworth, Paper submitted to the *Transactions of the American Mathematical Society*.
8. O. Ore, *Annals of Mathematics*, vol. 36 (1935), pp. 406-437.
9. A. De Morgan, *Trigonometry and Double Algebra*, p. 166.
10. R. E. Moritz, *Tohôku Journal*, vol. 21 (1921), pp. 51-64.