squares notation. In terms of the general equation of multiple regression, (I), the problem we have solved is that of the determination of the distribution of the regression coefficients b when it is supposed that the standard deviation of the dependent variate y is neither constant nor known for different sets $x_1 \ldots x_p$, but that the ratios of such standard deviations, for different sets, are known. When such ratios are all equal to unity, our problem simplifies into Fisher's—a problem which, while general enough for many valuable biological applications, has not been sufficiently general for application to the most frequently arising problems in practical physics and astronomy. The latter lead to systems of equations of condition, like (1), in which there is usually no unknown whose coefficient (even in the original, unweighted, equations) is the same in all the equations; they do not in general lead to systems of equations of the form (I).

[1] Legendre, *Nouvelles Méthodes pour la Détermination des Orbites des Comètes*, p. 72, Paris (1806).

[2] Gauss, *Theoria Motus Corporum Coelestium*, S. 177, Hamburg (1809); *Theoria Combinationis Observationum Erroribus Minimis Obnoxiae*, Werke, **4**, p. 1, Göttingen (1873).

[3] Laplace, *Théorie Anal. des Prob.*, **2**, Chap. 4 (1812).

[4] If one doubts the validity of geometrical reasoning, it is easy to recast the above argument into a purely analytical form.

[5] It is seen that s' is not correlated with any of the x''s, but that there is normal correlation between the x''s.

[6] After these results were obtained, they were compared with those of Jeffreys (*Proc. Roy. Soc.*, **A138,** 48 (1932)) and found to be the same. Jeffreys, however, obtained his results merely by an arbitrary choice of the distribution $p(\sigma)d\sigma \propto d\sigma/\sigma$ for σ, regardless of the sample; and the defective nature of that procedure was shown by Fisher (*Proc. Roy. Soc.*, **A139,** 343 (1933)) and Bartlett (*Proc. Roy. Soc.*, **A141,** 518 (1933)), all of whose objections are met by the treatment given here.

IDEALS IN ALGEBRAIC RINGS

BY GARRETT BIRKHOFF*

HARVARD UNIVERSITY

Communicated October 15, 1934

1. *Reduction by Ordinary Primes.*—This paper is a study of factorization in algebraic rings, and outlines a very direct attack which goes deep into the problem. Among other things, it shows that the divisibility (or "ideal") structure of an algebraic ring is either entirely canonical or very irregular. It further gives an arithmetic criterion for determining which algebraic integers give rise to canonical ideal structure.

For brevity, detailed proofs are omitted; of course they have been constructed. For brevity also, the nomenclature and notation of footnote 1 will be used without explanation.

Now let x be any algebraic integer, and let

$$f(x) = x^n + a_1x^{n-1} + a_2x^{n-2} + \ldots + a_n = 0 \qquad (1)$$

be the irreducible equation for x. The rational integers and x generate a ring R, and we shall denote by $L(R)$ the system whose elements are the non-zero ideals A, B, C, ... of R, and whose operations are g.c.f., l.c.m., product and ideal quotient. R and $L(R)$ are thoroughly familiar concepts to algebraists, and will be fixed throughout the paper.

By the "index" of an ideal $A \epsilon L(R)$ we mean the order of the residue ring R/A. Any A must contain a rational integer $a \neq 0$, and so must have a finite index dividing a^n. To every prime p consequently corresponds the system $L_p(R)$ of ideas whose index is a power of p.

Moreover it is true, although the proof is not easy, that $L(R)$ is essentially** the direct product of the $L_p(R)$. We can summarize this symbolically by writing

$$L(R) = L_2(R) \times L_3(R) \times L_5(R) \times \ldots \qquad (2)$$

and confine our attention to the various individual $L_p(R)$.

2. *Strong Isomorphism and Strong Semi-Isomorphism.*—Let $I \supset J$ and $K \supset L$ be any four ideals of R. A (1, 1) correspondence between the elements of the residue rings I/J and K/L will be called a "strong isomorphism" if and only if it preserves addition and multiplication, and is preserved under multiplication by an arbitrary $z \epsilon R$; it will be called a strong semi-isomorphism if and only if it preserves addition and is preserved under multiplication by an arbitrary $z \epsilon R$. In the first case we write $I/J \cong K/L$; in the second, $I/J \simeq K/L$.

THEOREM 1: If I, $J < I$ and $K < I$ are distinct ideals satisfying $(J, K) = I$, and if $I/J \simeq I/K$, then L exists, an ideal satisfying $(L, J) = (L, K) = I$ and $[L, J] = [L, K] = [J, K]$.

We form L from those residue classes $[J, K] + j + k$ of $[J, K]$ for which $j \epsilon J$ and $k \epsilon K$ correspond under the given strong semi-isomorphism.

3. *Irregular Case.*—The situation concerning the ideal of R/pR is totally clarified by the remark that we can apply Euclid's algorithm to polynomials modulo p, so that the ideals of R/pR correspond (1, 1) with the divisors of $f(x)$ modulo p which generate them. We now prove

THEOREM 2: Suppose that $g^2(x)$ divides $f(x)$ modulo p, that $g(x)$ is irreducible modulo p, and yet that the ideal $g(x)R \not\supset pR\ (p^2)$. Then the ideals of R do not satisfy

$$[(J, K), (J, L)] = (J, [K, L]). \qquad (3)$$

Set $I = (g(x)R, pR)$, $J = (g(x)R, p^2R)$, and $K = (g^2(x)R\ pR)$. We obtain ideals satisfying the hypotheses of Theorem 1, and therefore satisfying $[(J, K), (J, L)] = (J, K) < J = (J, [K, L])$, contrary to (3).

4. *Canonical Case.*—It can be proved that if $g^2(x)$ does not divide $f(x)$ modulo p while $g(x)$ is an irreducible factor of $f(x)$ modulo p, then $(g(x)R, pR)$ is a principal ideal generated by some $g(x) + kp\ (p)$. But if $g(x)R \supset pR(p^2)$, then $(g(x)R, pR)$ is a principal ideal, modulo any p^n. Finally, it is true that every largest ideal of $L_p(R)$ contains pR. Consequently, applying paragraph one of §3, we see that unless the hypotheses of Theorem 2 are satisfied for some $g(x)$, every largest ideal of $L_p(R)$ is a principal ideal, modulo any p^n.

But it can be proved that if T is a principal ideal in $L_p(R)$, then the transformation $I \longrightarrow TI$ carries $L_p(R)$ into the subsystem of ideals contained in T, isomorphically relative to g.c.f. and l.c.m. Using induction on index, we obtain

THEOREM 3: If no $g(x)$ satisfies the hypotheses of Theorem 2, then $L_p(R)$ is "canonical"—that is, isomorphic with the system of the products of a set of ordinary primes, relative to g.c.f., l.c.m., product and quotient.

5. *Consequences.*—Now we use our relation (2) to pass from $L_p(R)$ to $L(R)$. But we first note that any canonical system of ideals is "regular" in the sense of Grobner[3]—that is, that if $A \subset B$, then $A : (A : B) = B$—and that by Theorem 8 of footnote 2 any "regular" system of ideals satisfies (3). Therefore

THEOREM 4: The properties of satisfying (3), of being regular and of being canonical, are effectively equivalent in R, and all are equivalent to the property that if $g(x)$ is any irreducible factor of $f(x)$ modulo p, then either $g^2(x)$ does not divide $f(x)$ modulo p, or else $(g(x)R, p^2R) \supset pR$.

The author intends to publish elsewhere complete proofs of the assertions made above, together with related theorems and applications to the arithmetics of specific algebras. As an example of the results proved, we shall cite

THEOREM 5: The number of different simple factors J/K in $L_p(R)$ relative to strong isomorphism, is twice the number of irreducible factors of $f(x)$ modulo p.

* Society of Fellows, Harvard University.

** Technically, the "subdirect product" in the sense of footnote 2, §3.

[1] O. Ore, "Abstract Ideal Theory," *Bull. Am. Math. Soc.*, **39**, 728–45 (1933).

[2] G. Birkhoff, "On the Lattice Theory of Ideals," *Ibid.*, **40**, 613–19 (1934).

[3] W. Grobner, "Uber irreduziblen Ideale in kommutativen Ringe," *Math. Ann.*, **110**, 161–94 (1934).