UNIQUE FACTORIZATION

PIERRE SAMUEL, Institut Henri Poincaré, Paris

1. Introduction. It is well known that every ordinary integer is, in a unique way, a product of prime numbers. With an eye to generalizations it is better to state this unique factorization property in the *ring* Z of rational (i.e., >0 or <0) integers. Thus, if we denote by P the set of all prime numbers, every nonzero element x of Z may be written, in a unique way, as

$$x = \pm 1 \prod_{p \in P} p^{\nu_p(x)}, \tag{1}$$

where the exponents $\nu_p(x)$ are positive integers, almost all 0 (i.e., equal to 0 except for a finite number of them) in order that formula (1) makes sense. The somewhat abstract formulation given by (1), with its seemingly infinite product, has the great advantage of indicating how the exponents $\nu_p(x)$ depend on x. If we allow negative exponents, we see that (1) holds also for all *nonzero* rational numbers x. Furthermore, for any pair x,y of nonzero rational numbers, we see that we have

$$\nu_p(xy) = \nu_p(x) + \nu_p(y), \qquad \nu_p(x+y) \geqq \inf(\nu_p(x), \nu_p(y)). \tag{2}$$

Algebraists express formulae (2) by saying that the mapping $\nu_p \colon Q^* \to Z$ is a *discrete valuation* of the field of rational numbers.

More generally, we define a *factorial ring* (or a "unique factorization domain," U.F.D.) to be an integral domain A for which there exists a subset P of A such that every nonzero element x of A may be written, in a *unique* way, as

$$x = u \prod_{p \in P} p^{\nu_p(x)} \tag{1'}$$

where u is a *unit* (i.e., an invertible element) in A, and where the exponents $\nu_p(x)$ are positive integers, almost all 0. It can easily be proved that the subset P is uniquely determined up to units; more precisely the set $(Ap)_{p \in P}$ of principal ideals is uniquely determined, and coincides with the set of all maximal principal ideals distinct from A. Let us notice that a principal ideal Ab of a domain A is maximal (among principal ideals distinct from A) iff every divisor d of b is either a unit or is such that db^{-1} is a unit; such an element b is called an *irreducible* element of A.

For a ring A, factoriality is a very useful property. At least for multiplicative questions, the *arithmetic* in a factorial ring A is as nice as in the ring Z of ordinary integers. It may be recalled that, in the 19th century, arithmeticians like Kummer and Dedekind noticed that some rings of algebraic integers failed to be factorial; e.g., the formulae

$$2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5}), \qquad 3 \cdot 3 = (\sqrt{10} + 1)(\sqrt{10} - 1)$$

show that the rings $Z[\sqrt{-5}]$, $Z[\sqrt{10}]$ are not factorial; this led Kummer and

Dedekind to introduce the important notion of an *ideal*, and to replace the unique factorization of elements by the unique factorization of ideals, thus inaugurating the theory of rings which we now call "Dedekind rings." Lack of time prevents me from talking more about this important and beautiful theory.

The interest of factorial rings does not come only from arithmetical reasons. Factoriality has also a very simple *geometric* interpretation. In geometry, more precisely in the study of algebraic, analytic or formal varieties, a ring A occurs as a ring of functions (algebraic or analytic, as the case may be) on some variety V, or in the neighborhood of some point of V. To say that A is a domain means that V is irreducible. Denoting by n the dimension of V, the factoriality of A then means, roughly speaking, that every subvariety of W of dimension $n-1$ of V may be defined *by a single equation*; more precisely the functions $f \in A$ which vanish on W form an ideal $p(W)$ in A, and factoriality means that these ideals $p(W)$ (for dim $W = n-1$) are principal.

2. How to prove factoriality. We have just seen that factoriality is a desirable property for a ring. On the other hand proving that a ring is factorial is rarely trivial, so it is useful to have at hand as many characterizations of factorial rings as possible.

As we have seen in Section 1, factoriality of A means that every nonzero element of A admits a decomposition as a product of irreducible ones, and that this decomposition is unique up to units. The existence of such a decomposition is usually easy to check; it follows from this "chain condition" for principal ideals (valid in any factorial ring):

(3) *Every strictly increasing sequence of principal ideals of A is finite*, which is itself equivalent to the "maximal condition":

(3′) *Every nonempty family of principal ideals of A admits a maximal element.*

For example (3) (or (3′)) holds when the ring A is noetherian, and most rings that are encountered in arithmetic or in geometry are noetherian. Furthermore, with proper caution, property (3) may pass to the direct limits. We henceforth assume that (3) holds.

As to *uniqueness*, things are not so easy. Unique factorization in a ring A implies that any irreducible element p of A enjoys the stronger property that

(4) *If p divides a product ab, then it divides a or b.*

Conversely, assuming (3), a well-known proof copied from elementary number-theory shows that (4) implies the uniqueness of the decomposition into irreducible factors. An element p which enjoys property (4) is called a *prime* element of A; this means that the principal ideal Ap is a prime ideal ($ab \in Ap \Rightarrow a \in Ap$ or $b \in Ap$), or, equivalently, that the factor ring A/Ap is a domain. As shown in elementary number-theory, property (4) is equivalent to

(4′) *Any two elements of A admit a greatest common divisor*, and also to:

(4″) *Any two elements of A admit a least common multiple.*

A rather handy form of (4″) is

(4‴) *The intersection of any two principal ideals of A is a principal ideal.*

If we deal with a *noetherian* domain A, it can be proved that every nonunit in A is contained in a prime ideal of height 1 (i.e., a prime ideal which is minimal among nonzero prime ideals). From this one easily deduces that a noetherian domain A is factorial iff

(5) *Every prime ideal of height* 1 *of A is principal.*

This condition has already been met at the end of Section 1, when we discussed the geometric meaning of factoriality.

More technical characterizations of factorial rings may be given in the framework of the theory of *Krull rings*, for which we refer to Bourbaki, "Algèbre Commutative," Chap. VII, "Diviseurs" [4]. Let us only say that the class of Krull rings contains the class of factorial rings and is more stable under various ring-theoretic operations. Furthermore, it is in general easy to test whether a given ring is a Krull ring or not. The problem is therefore to test whether a given Krull ring is factorial, and, if not, to measure its "nonfactoriality."

3. Properties stronger than factoriality. For proving that Z is factorial, one usually first proves that Z is *principal* (i.e., that every ideal of Z is principal). Then the chain condition (3) is very easy, and condition (4‴) is obvious. The example of a polynomial ring in several variables over a field shows that being principal is a stronger property than being factorial; thus it could seem to be dangerous to concentrate on this stronger property for proving factoriality. However, we have a reliable touchstone for telling us whether the danger exists or not. In fact the commutative algebraists have developed an extensive theory of the *dimension* of a ring, and many methods for computing the dimension of a ring are available. Moreover the principal rings are characterized as being the factorial rings of *dimension* 0 *or* 1. Thus the dimension of the ring A we are studying will tell us whether it is reasonable to attempt to prove that A is principal.

In most geometric cases, principality is proved by proving separately factoriality and one-dimensionality. But, in *algebraic number theory*, there are methods for proving directly that a ring is principal. For instance, let K be a number-field of finite degree n over the rationals, let A be the ring of algebraic integers of K, d the absolute discriminant of A, and $2r_2$ the number of nonreal conjugates of K in C. Then, by using Minkowski's theory of lattice points in convex sets, one can prove that every nonzero ideal $\mathfrak{A}$ of A may be written as $\mathfrak{A}=xb$, where x is an element of K^* and where b is an ideal in A for which

$$\text{(6)} \qquad \operatorname{card}(A/b) < \left(\frac{4}{\pi}\right)^{r_2} \frac{n!}{n^n} (|d|^{1/2}).$$

Now the right hand side of (6) can be computed by standard methods, whereas the ideals b for which A/b has a given cardinal c are finite in number, and are easy to determine if c is not too large. Thus, if it happens that all the ideals b for which (6) is satisfied are principal, then the ring A is principal. The reader may apply the method to the ring $A=Z[i]$ of Gaussian integers (here $r=2$, $r_2=1$, $|d|=4$, whence the right hand side of (6) is <2, and (6) thus implies $b=A$); he may then feel that this is a very sophisticated method for proving that $Z[i]$ is principal! In fact the usual proof for $Z[i]$, as well as for Z or for a polynomial ring $k[X]$ over a field k, uses the fact that these rings are *euclidean*. Let us recall that an integral domain A is said to be euclidean if there exists a mapping $\phi: A\rightarrow N$ (the positive integers) such that, for every nonzero b in A, every class modulo Ab admits a representative r such that $\phi(r)<\phi(b)$ (i.e., every a in A may be written $a=bq+r$ with $\phi(r)<\phi(b)$). A euclidean ring A is principal for, given a nonzero ideal b in A, we choose a nonzero element x of b for which $\phi(x)$ is minimal, and see that x generates b. For this proof, it is not necessary to assume that ϕ takes its values in N; any well ordered set W would work as well. A mapping $\phi: A\rightarrow W$ satisfying the above property is called an algorithm on A. If we consider a given ring A and a large-enough well ordered set W (e.g., such that card $(W)>$card (A)), the theory of well ordered sets shows that every algorithm on A is isomorphic (in an obvious sense) with an algorithm with values in W. Furthermore, if $\phi_\alpha: A\rightarrow W$ is a family of algorithms on A, then $\phi=\inf_\alpha\phi_\alpha$ is also an algorithm, so that A (if euclidean) admits a smallest algorithm. If the residue fields of A are finite, this smallest algorithm ϕ_0 actually takes its values in N (the general case is still open). But it is not necessarily the usual algorithm: in the case of Z, $\phi_0(n)$ is the number of binary digits of the integer $|n|$ $(n\in Z)$; however, for polynomials in X over a field k, $\phi_0(P(X))$ is the degree of the polynomial $P(X)$.

Much work has been done by arithmeticians for determining the number fields for which the ring A of integers is euclidean; most of them studied the more restricted problem of finding out whether the usual "norm-function" (i.e., $\phi(x)=$card (A/Ax) for $x\neq 0$) is an algorithm or not. For imaginary quadratic fields, the five fields Q $(\sqrt{-d})$ for $d=1, 2, 3, 7, 11$ are the only ones for which the norm is an algorithm, and are also the only euclidean ones. But there are four principal noneuclidean rings of integers in imaginary quadratic fields for $d=19$, 47, 67 and 163 (the problematic existence of a fifth one has recently been disproved). As to real quadratic fields Q $(\sqrt{m})$ $(m>0)$, the list of those which are euclidean for the norm is known:

$$m = 2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73.$$

Many others are known to be principal, but we do not know whether their number is finite or not. Also we do not know whether some of them might not be euclidean for another algorithm than the norm; a bit of evidence induces the writer to think that $Q(\sqrt{14})$ deserves to be studied in this respect (see [5], [6]). Summarizing, one might say that the theory of euclidean rings has a quite different flavor from that of factoriality.

4. Nagata's Theorem. Masayoshi Nagata has proved a theorem which is very useful for showing that a ring is factorial. We recall that, if A is an integral domain with quotient field K and if S is a multiplicatively closed subset of $A (0 \notin S)$, then the fractions a/s with $a \in A$ and $s \in S$ form a subring of K, denoted by $S^{-1}A$, and called the *ring of quotients* of A with respect to S. Now suppose that A satisfies the finiteness condition (3) (see Section 2), that S is generated by *prime* elements (Section 2), and that $S^{-1}A$ is factorial; then Nagata's theorem states that A itself is *factorial.* If S is generated by a finite number of prime elements, one can dispense with condition (3). A very easy converse of Nagata's theorem is that any ring of quotients of a factorial ring is factorial.

Gauss's lemma about *polynomial rings* is an easy consequence of Nagata's theorem. In fact let R be a factorial ring, L its quotient field, and $S = R - \{0\}$. Since a prime element p of R remains prime in the polynomial ring $A = R[X]$ (for $A/pA = (R/pR)[X]$ is a domain), S is generated by prime elements of A. But $S^{-1}A = L[X]$ is a polynomial ring in one variable over a field, whence is euclidean and factorial. Hence $A = R[X]$ is factorial by Nagata. By induction the same holds for polynomial rings in several variables over a factorial ring.

Let us sketch three other *examples* of application of Nagata's theorem (complete proofs are left to the reader):

(a) Let k be an algebraically closed field of characteristic $\neq 2$, and $F(X_1, \cdots, X_n)$ a nondegenerate quadratic form over k, with $n \geqq 5$. Then $A = k[X_1, \cdots, X_n]/(F)$ is factorial. (By a change of variables, write $F = X_1X_2 + G(X_3, \cdots, X_n)$; denote by x_j the image of X_j in A; then x_1 is prime since G is irreducible (for $n \geqq 5$); taking $S = \{1, x_1, \cdots, x_1^j, \cdots\}$, we see that $S^{-1}A = k[x_1, x_3, \cdots, x_n][1/x_1]$ is factorial as a ring of quotients of a polynomial ring.)

(b) Let k be a field in which -1 is not a square, and $A = k[X, Y, Z]/(X^2 + Y^2 + Z^2 - 1)$ ("the ring of the 2-sphere"); then A is factorial. (Denote by x, y, z the images of X, Y, Z in A; then $x^2 + y^2 = (1+z)(1-z)$; take S generated by $1-z$, which is prime; now $S^{-1}A$ is factorial as in (a).)

(c) Let k be a field and $A = k[X, Y, Z]/(X^r + Y^s + Z^t)$ where the exponents r, s, t are pairwise relatively prime; then A is factorial. (Denote by x, y, z the images of X, Y, Z in A, so that $z^t = -(x^r + y^s)$; suppose first that $t \equiv 1 \pmod{rs}$, i.e., $t = 1 + drs$; take S generated by z (which is prime), and set $x' = x/z^{ds}$, $y' = y/z^{dr}$; then $z = -(x'^r + y'^s)$ and $S^{-1}A = k[x', y'][1/z]$ is factorial; in the general case, one chooses an integer j such that $jt \equiv 1 \pmod{rs}$, and replaces z by some jth root w of z.)

5. Further Results. The theory of factorial rings is nowadays much more developed than has been sketched above. For example, in [2] of the bibliography, we find about 80 pages of lecture notes entirely devoted to factoriality with sizeable prerequisites from commutative and homological algebra; moreover these notes did not contain everything known on the subject when they were written (1963), and the theory has progressed since that time. We will thus briefly sketch some highlights of this theory, without defining some of the terms we use; for detailed definitions, proofs and connected results, we refer the reader to the bibliography.

(1) *Power Series.* In Section 4 we have stated Gauss's lemma about polynomial rings. It is a particular instance of the "transfer" of some property from a ring A to the polynomial ring $A[X]$. Many similar transfers are known, and also transfers of properties from a ring A to the formal power series ring $A[[X]]$. Thus it was reasonable to conjecture that, if A is factorial, so is $A[[X]]$. This conjecture has been disproved (see [7]). In the first counter-examples given, the ground ring A was a noncomplete local ring, and taking formal power series over a noncomplete local ring could be deemed, by some mathematicians, to be an unnatural (or even immoral) operation. Doubts were settled very recently by P. Salmon [13], who constructed a complete local factorial ring A such that $A[[X]]$ is not factorial.

(2) *Regular Rings.* The notion of a regular ring is defined in commutative algebra; in the geometric case, it corresponds to the notion of a nonsingular variety. In 1957, M. Auslander and D. Buchsbaum proved, by homological methods, that any regular local ring is factorial. Their proof has been streamlined by I. Kaplansky [1], [2], and by N. Bourbaki [4].

On the other hand, if A is a regular and factorial ring (not necessarily local), then both $A[X]$ and $A[[X]]$ are factorial.

(3) *Galoisian going-down.* Let A be a factorial ring, and G a finite group of automorphisms of A; the elements of A which are invariant by G form a subring of A, traditionally denoted by A^G. Let A^* be the multiplicative group of units A. Then if the cohomology group $H^1(G, A^*)$ vanishes, the ring A^G is factorial ([2], [3], [17]).

Here the writer cannot resist giving an amusing example. We take for A a polynomial ring $A = k[X_1, \cdots, X_n]$ (k: a field, $n \geqq 5$), and for G the *alternating group* A_n, acting on A by permutations of the variables. Here the ring of invariants A^G is generated over k by the elementary symmetric functions $s_1, \cdots, s_n$ and by the "discriminant" $d = \Pi_{i<j}(X_i - X_j)$; it is known that $d^2 = P(s_1, \cdots, s_n)$ where P is a polynomial over k. Furthermore $A^* = k^*$ is trivially operated by G, so that $H^1(G, A^*) = \text{Hom}(G, k^*)$ (classical formula in the cohomology of groups). Since $G = A_n$ is a simple group ($r \geqq 5$) and since k^* is commutative, we have $\text{Hom}(G, k^*) = 0$ and A^G is factorial.

The same method has given an example of a factorial ring which is not a Macaulay ring [18]. Notice that P. Murthy has proved that a factorial Macaulay ring is necessarily a Gorenstein ring.

In characteristic $p \neq 0$, there is a parallel theory in which automorphisms are replaced by derivatives ([2], [9], [16]). As above the proofs of factoriality are partly computational, and (especially in characteristic 2) the complete performance of these computations is sometimes more accessible than in the case of automorphisms.

(4) *Complete Intersections.* A local ring A is called a "complete intersection" if it is isomorphic to some R/I, where R is a regular local ring and I an ideal

generated by a regular R-sequence (this means that I may be generated by $\dim(R)-\dim(R/I)$ elements). By using powerful methods of his theory of schemes (the latest version of algebraic geometry), A. Grothendieck proved that a complete intersection A, such that A_p is factorial whenever $\dim(A_p)\leqq 3$, is itself factorial ([19]). This generalizes older geometric theorems of F. Severi, S. Lefshetz and A. Andreotti. No purely ring-theoretic proof of Grothendieck's theorem is known.

(5) *Two-dimensional Factorial Rings.* We have already said that the factorial rings of dimension one are the principal rings; among them, the local ones are the discrete valuation rings and are considered as well known. In dimension 2, we have already seen a good number of examples of factorial rings: e.g., the rings of the surfaces $x^i+y^j+z^k=0$ (i, j, k pairwise relatively prime) and of the sphere $x^2+y^2+z^2-1=0$; localizing the first ones at the origin, we obtain many non-regular local factorial rings of dimension 2. These local rings are not complete and, moreover, the factoriality of their completions $C=K[[x, y, z]]$ was in doubt. First G. Scheja and D. Mumford proved that the complete ring C of the surface $x^2+y^3+z^5=0$ is factorial. Then P. Salmon, for the counterexample alluded to in (1), proved the same for the surface $x^2+y^3+tz^6=0$ over a field K of the form $K=k(t)$ with t transcendental over k.

In this last example the ground field K is not algebraically closed. Now E. Brieskorn, by using techniques from algebraic geometry, has proved that, among the complete two-dimensional local rings over an algebraically closed field K, only two are factorial: the regular ring $K[[X, Y]]$ (formal power series), and the ring $K[[x, y, z]]$ with $x^2+y^3+z^5=0$ (cf. [13]). It can be noted that the latter is the ring of invariants of an icosahedral group acting on the former [1].

A bibliography of factorial rings

An elementary exposition can be found in:

1. P. Samuel, Anneaux Factoriels (red. A. Micali), Bol. Soc. Mat., São Paulo, 1964.

More complete results in:

2. P. Samuel, Lectures on unique factorization domains, (notes by Pavman Murthy) Tata Institute for Fundamental Research lectures, No. 30, Bombay, 1964.

3. ———, Lectures in commutative algebra (notes by M. Bridger), mimeographed by Brandeis University, Waltham, Mass., 1964–65 (write to Brandeis).

For a treatment of factorial rings, in the framework of Krull rings, see:

4. N. Bourbaki, Algèbre Commutative, Chap. VII "Diviseurs," Hermann, Paris, 1966.

For the case of number-fields, see:

5. Hardy-Wright, An introduction to the theory of numbers, Clarendon, Oxford, 1960, and also the tables in

6. Borovič-Safarevič, Théorie des nombres, Gauthier-Villars, Paris, 1966. (German and English translations also available.)

Most results, up to 1964, about factorial rings are given in [1], [2], [3]. For the reader's convenience, we however quote:

7. P. Samuel, On unique factorization domains, Ill. J. Math., 5 (1961) 1–17.

8. ———, Sur les anneaux factoriels, Bull. SMF, 89 (1961) 155–173.

9. ———, Classes de diviseurs et dérivées logarithmiques, Topology, 3, Supp. 1 (1964) 81–96.

10. ———, Modules réflexifs et anneaux factoriels, In Colloque International de Clermont-Ferrand, ed. CNRS, Paris, 1965.

11. P. Samuel, Sur les séries formelles restreintes, C.R. Acad. Sci., Paris, 1962.

The ring of the surface $x^2+y^3+z^5=0$ is studied in

12. F. Klein, Lectures on the icosahedron, Dover, New York, 1956, Chap. 2, Sections 12 and 13.

13. E. Brieskorn, Local rings which are UFD's, (preprint, MIT, Oct. 1966), and in articles of G. Scheja (Math. Ann., 1965), and D. Mumford (Publ. I.H.E.S., 9 (1961)).

The first example of a complete local ring A for which $A[[t]]$ is not factorial was given in:

14. P. Salmon, Sulla non-factorialita . . . , Rend. Lincei, June 1966.

A further discussion of this example is in:

15. N. Zinn-Justin, Dérivations des corps et anneaux de caractéristique p, (Thèse Paris 1967); in print in Mémoires Soc. Math. France, 1967.

For the theory of the "purely inseparable going-down," see:

16. N. Hallier, Utilisation des groupes de cohomologie dans la théorie de la descente p-radicielle, C.R. Acad. Sci. Paris, 261 (1965) 3922–3924, and also [15]. (NB: Hallier is the maiden-name of Mrs. Zinn-Justin.)

For examples of "galoisian going-down," see:

17. M. J. Dumas, Sous anneaux d'invariants d'anneaux de polynômes, C.R. Acad. Sci. Paris, 260 (1965) 5655–5658.

18. M. J. Bertin, Sous groupes cycliques d'ordre $p^n \cdots$, C.R. Acad. Sci. Paris, April 1967. (NB: Dumas is the maiden-name of Mrs. Bertin.)

A proof of Grothendieck's theorem on the factoriality of some complete intersections is in

19. A. Grothendieck, Séminaire de Géometrie Algébrique 1961–1962, exposé XI, mimeographed by the Institut des Hautes Etudes Scientifiques, 35 route de Chartres, 92-Bures sur Yvette. France.

SOME GENERALIZED "ISOMOMENT" EQUATIONS AND THEIR GENERAL SOLUTIONS

J. ACZEL, University of Waterloo, Ontario, Canada, and P. FISCHER,
Automatizálási Kutató Intézet, Budapest, Hungary

1. Introduction. In a previous paper [3] one of us has proved that *all real solutions of the* "isomoment" (terminology of S. Kotz [8]) *functional equation*

$$f\left(\sum_{k=1}^{n} x_k^m/n\right) = \sum_{k=1}^{n} f(x_k)^m/n \tag{1}$$

satisfied for all

$$x_k \geqq 0 \tag{2}$$

($k=1, 2, \cdots, n$) and for fixed integers $n>1$, $m>1$ *are continuous and given by*

$$f(x) = 0, \tag{3_t}$$

$$f(x) = 1, \qquad f(x) = x \tag{3_i}$$

in case of any integer $m>1$, *and* further

$$f(x) = -1, \qquad f(x) = -x \tag{3_o}$$

in case of odd $m>1$.