Oscar Zariski · Pierre Samuel

Commutative Algebra

Volume 1

With the cooperation of

I. S. Cohen

Springer-Verlag New York Heidelberg Berlin
World Publishing Corporation, Beijing, China

Oscar Zariski
Harvard University
Department of Mathematics
Cambridge, Massachusetts 02138

Pierre Samuel
Université de Paris-Sud
Mathématique/Bâtiment 425
91405 Orsay, France

AMS Subject Classifications
13-01, 13AXX, 13BXX, 13CXX, 13E05, 13F05, 13F10

Library of Congress Cataloging in Publication Data

Zariski, Oscar, 1899–
Commutative algebra.
(Graduate texts in mathematics; v. 28)
Reprint of the 1958–1960 ed. published by Van Nostrand, Princeton, N.J., in series: The University series in higher mathematics, edited by M. H. Stone, D. C. Spencer, H. Whitney, and O. Zariski.
Includes index.
1. Commutative algebra. I. Samuel, Pierre, 1921– joint author. II. Series: Graduate texts in mathematics; v. 28–
QA251.3.Z37 1975 512'.24 75-17751

ISBN 0-387-90089-6 Springer-Verlag New York Heidelberg Berlin
ISBN 3-540-90089-6 Springer-Verlag Berlin Heidelberg New York
ISBN 7-5062-0058-9 World Publishing Corporation China

PREFACE

Le juge: Accusé, vous tâcherez d'être bref.
L'accusé: Je tâcherai d'être clair.

—G. COURTELINE

This book is the child of an unborn parent. Some years ago the senior author began the preparation of a Colloquium volume on algebraic geometry, and he was then faced with the difficult task of incorporating in that volume the vast amount of purely algebraic material which is needed in abstract algebraic geometry. The original plan was to insert, from time to time, algebraic digressions in which concepts and results from commutative algebra were to be developed in full as and when they were needed. However, it soon became apparent that such a parenthetical treatment of the purely algebraic topics, covering a wide range of commutative algebra, would impose artificial bounds on the manner, depth, and degree of generality with which these topics could be treated. As is well known, abstract algebraic geometry has been recently not only the main field of applications of commutative algebra but also the principal incentive of new research in commutative algebra. To approach the underlying algebra only in a strictly utilitarian, auxiliary, and parenthetical manner, to stop short of going further afield where the applications of algebra to algebraic geometry stop and the general algebraic theories inspired by geometry begin, impressed us increasingly as being a program scientifically too narrow and psychologically frustrating, not to mention the distracting effect that repeated algebraic digressions would inevitably have had on the reader, vis-à-vis the central algebro-geometric theme. Thus the idea of a separate book on commutative algebra was born, and the present book—of which this is the first of two volumes—is a realization of this idea, come to fruition at a time when its parent—a treatise on abstract algebraic geometry—has still to see the light of the day.

In the last twenty years commutative algebra has undergone an intensive development. However, to the best of our knowledge, no systematic account of this subject has been published in book form since the appearance in 1935 of the valuable *Ergebnisse* monograph "Idealtheorie" of

W. Krull. As to that monograph, it has exercised a great influence on research in the intervening years, but the condensed and sketchy character of the exposition (which was due to limitation of space in the *Ergebnisse* monographs) made it more valuable to the expert than to the student wishing to study the subject. In the present book we endeavor to give a systematic and—we may even say—leisurely account of commutative algebra, including some of the more recent developments in this field, without pretending, however, to give an encyclopedic account of the subject matter. We have preferred to write a self-contained book which could be used in a basic graduate course of modern algebra. It is also with an eye to the student that we have tried to give full and detailed explanations in the proofs, and we feel that we owe no apology to the mature mathematician, who can skip the details that are not necessary for him. We have even found that the policy of trading empty space for clarity and explicitness of the proofs has saved us, the authors, from a number of erroneous conclusions at the more advanced stages of the book. We have also tried, this time with an eye to both the student and the mature mathematician, to give a many-sided treatment of our topics, not hesitating to offer several proofs of one and the same result when we thought that something might be learned, as to methods, from each of the proofs.

The algebro-geometric origin and motivation of the book will become more evident in the second volume (which will deal with valuation theory, polynomial and power series rings, and local algebra; more will be said of that volume in its preface) than they are in this first volume. Here we develop the elements of commutative algebra which we deem to be of general and basic character. In chapter I we develop the introductory notions concerning groups, rings, fields, polynomial rings, and vector spaces. All this, except perhaps a somewhat detailed discussion of quotient rings with respect to multiplicative systems, is material which is usually given in an intermediate algebra course and is often briefly reviewed in the beginning of an advanced graduate course. The exposition of field theory given in chapter II is fairly complete and follows essentially the lines of standard modern accounts of the subject. However, as could be expected from algebraic geometers, we also stress treatment of transcendental extensions, especially of the notions of separability and linear disjointness (the latter being due to A. Weil). The study of maximally algebraic subfields and regular extensions has been postponed, however, to Volume II (chapter VII), since that study is so closely related to the question of ground field extension in polynomial rings.

Chapter III contains classical material about ideals and modules in arbitrary commutative rings. Direct sum decompositions are studied in detail. The last two sections deal respectively with tensor products of rings and free joins of integral domains. Here we introduce the notion of quasi-linear disjointness, and prove some results about free joins of integral domains which we could not readily locate in the literature.

With chapter IV, devoted to noetherian rings, we enter commutative algebra proper. After a preliminary section on the Hilbert basis theorem and a side trip to the rings satisfying the descending chain condition, the first part of the chapter is devoted mostly to the notion of a primary representation of an ideal and to applications of that notion. We then give a detailed study of quotient rings (as generalized by Chevalley and Uzkov). The end of the chapter contains miscellaneous complements, the most important of which is Krull's theory of prime ideal chains in noetherian rings. An appendix generalizes some properties of the primary representation to the case of noetherian modules.

Chapter V begins with a study of integral dependence (a subject which is nowadays an essential prerequisite for almost everything in commutative algebra) and includes the so-called "going-up" and "going-down" theorems of Cohen-Seidenberg and the normalization theorem. (Other variations of that theorem will be found in Volume II, in the chapter on polynomial and power series rings.) With Matusita we then define a Dedekind domain as an integral domain in which every ideal is a product of prime ideals and derive from that definition the usual characterization of Dedekind domains and their properties. An important place is given to the study of finite algebraic field extensions of the quotient field of a Dedekind domain, and the degree formula $\Sigma e_i f_i = n$ is derived under the usual (and necessary) finiteness assumptions concerning the integral closure of the given Dedekind domain in the extension field. This study finds its natural refinement in the Hilbert ramification theory (sections 9 and 10) and in the properties of the different and discriminant (section 11). The chapter closes with some classical number-theoretic applications and a generalization of the theorem of Kummer. The properties of Dedekind domains give us a natural opportunity of introducing the notion of a valuation (at least in the discrete case) but the reader will observe that this notion is introduced by us quite casually and parenthetically, and that the language of valuations is not used in this chapter. We have done that deliberately for we wished to emphasize the by now well-known fact that while ideals and valuations cover substantially the same ground in the classical case (which, from a geometric point of view, is the case of dimension 1), the

domain in which valuations become really significant belongs to the theory of function fields of dimension greater than 1.

The preparation of the first volume of this book began as a collaboration between the senior author and our former pupil and friend, the late Irving S. Cohen. We extend a grateful thought to the memory of this gifted young mathematician.

We wish to acknowledge many improvements in this book which are due to John Tate and Jean-Pierre Serre. We also wish to thank heartily Mr. T. Knapp who has carefully read the manuscript and the galley proofs and whose constructive criticisms have been most helpful.

Thanks are also due to the Harvard Foundation for Advanced Research whose grant to the senior author was used for typing part of the manuscript. Last but not least, we wish to extend our thanks to the D. Van Nostrand Company for having generously cooperated with our wishes in the course of the printing of the book.*

PREFACE TO THE SPRINGER EDITION

In this edition the most important change is the formulation and strengthening of Theorem 29 (p. 303) and corresponding changes in the proof of that theorem (pp. 304–305). The chief purpose of this change is to have in this volume an explicit statement of the very useful formula $f'_y = \mathfrak{D}_x$ for extensions of Dedekind domains and the full proof of this theorem. Besides this, several minor misprints have been corrected.

* The work on this volume was supported in part by a research project at Harvard University, sponsored by the Office of Ordnance Research, United States Army, under Contract DA-19-020-ORD-3100.

TABLE OF CONTENTS

I. INTRODUCTORY CONCEPTS

§ 1. Binary operations. Let G be an arbitrary set of elements $a, b, c, \cdots$. By a *binary operation in* G is meant a rule which associates with each *ordered* pair (a, b) of elements of G a unique element c of the same set G. A binary operation can therefore be thought of as a single-valued function whose domain is the set of all ordered pairs (a, b) of elements of G and whose range is either G itself or some subset of G. We point out explicitly that if a and b are *distinct* elements of G, then the elements of G which are associated with the ordered pairs (a, b) and (b, a) may very well be distinct.

In group theory, and in algebra generally, it is customary to denote by $a \cdot b$ or ab the element which is associated with (a, b) under a given binary operation. The element $c = ab$ is then called the *product* of a and b, and the binary operation itself is called *multiplication*. When the term "multiplication" is used for a binary operation, it carries with it the implication that "*if* $a \in G$ (read: a is an element of G) *and* $b \in G$, *then also* $ab \in G$." We shall often express this property by saying that G *is closed under the given multiplication.*

Let G be a set on which there is given a binary operation, which we write as multiplication. The operation is said to be *associative* if $(ab)c = a(bc)$ for any three elements a, b, c of G. Two elements a and b of G are said to *commute* if $ab = ba$, and the operation is said to be *commutative* if any two elements of G commute.

We assume henceforth that the operation in question is associative. It is then a simple matter to define inductively the powers of an element of G and to prove the usual rules of exponents. Namely, if $a \in G$ and if n is a positive integer, we define $a^1 = a$; if $n > 1$, $a^n = a^{n-1}a$. We then have for any positive integers m and n:

$$a^m a^n = a^{m+n}; \tag{1}$$

$$(a^m)^n = a^{mn}. \tag{2}$$

For fixed m, one can proceed by induction on n, observing that these

rules hold by definition for $n = 1$. Moreover, if a and b are two elements of G which commute, then so do any powers of a and b, and

$$(ab)^n = a^n b^n. \tag{3}$$

An *identity element* in G is an element e in G such that $ea = ae = a$ for all a in G. If G has an identity e, then it has no other. For if e' is also an identity, then $e = ee' = e'$. Moreover, we can now define a^0 to be e, and the foregoing three rules trivially hold for arbitrary non-negative exponents.

We now assume that G has an identity e. If $a \in G$, an *inverse* of a is an element a' in G such that $a'a = aa' = e$. If a'' is also an inverse of a, then $a'' = a''e = a''(aa') = (a''a)a' = ea' = a'$. Thus the inverse of a (if it exists at all) is unique. If a possesses an inverse a', then negative powers of a can also be defined. Namely, we observe that

$$a^m = a^{m+1}a'$$

for all non-negative m, and we take this as an inductive definition for negative m. Thus $a^m a = a^{m+1}$ for *all* m. The rule (1) above is then true for any fixed m (positive or negative), provided $n = 1$; it can be proved for arbitrary positive n by induction from $n - 1$ to n and for negative n by induction from $n + 1$ to n. Since, therefore, $a^m a^{-m} = e = a^{-m}a^m$, we observe that a^m has a^{-m} as inverse, so that $(a^m)^n$ is defined for every n. Rule (2) can now be proved by the two inductions used for (1). From the definition we have that $a^{-1} = a'$, and we shall always use a^{-1} for the inverse of a (if it exists). If a and b both have inverses, then so does ab, and $(ab)^{-1} = b^{-1}a^{-1}$. If, moreover, a and b commute, then so do any powers of a and b, and (3) holds for arbitrary n.

The product of n elements $a_1, \cdots, a_n$ of G is inductively defined as follows:

$$\prod_{i=1}^{n} a_i = a_1 \quad \text{if } n = 1; \qquad \prod_{i=1}^{n} a_i = \left(\prod_{i=1}^{n-1} a_i\right) a_n \quad \text{if } n > 1.$$

This product will be denoted also by $a_1 a_2 \cdots a_n$. From the associativity of multiplication in G, we can prove the following general associative law, which states that the value of a product is independent of the grouping of the factors:

Let $n_0, n_1, \cdots, n_r$ be integers such that $0 = n_0 < n_1 < \cdots < n_r = n$. Then

$$\prod_{j=1}^{r}\left(\prod_{k=n_{j-1}+1}^{n_j} a_k\right) = \prod_{i=1}^{n} a_i.$$

This is clear for $n = 1$; hence we assume it proved for $n - 1$ and

prove it for n factors. The formula being trivial for $r = 1$, we may assume $r > 1$. Then

$$\prod_{j=1}^{r}\Big(\prod_{k=n_{j-1}+1}^{n_j} a_k\Big)$$

$$= \Big[\prod_{j=1}^{r-1}\Big(\prod_{k=n_{j-1}+1}^{n_j} a_k\Big)\Big]\Big[\Big(\prod_{k=n_{r-1}+1}^{n_r-1} a_k\Big)a_n\Big] \quad \text{(by definition)}$$

$$= \Big\{\Big[\prod_{j=1}^{r-1}\Big(\prod_{k=n_{j-1}+1}^{n_j} a_k\Big)\Big]\Big[\prod_{k=n_{r-1}+1}^{n_r-1} a_k\Big]\Big\}a_n \quad \text{(by associativity)}$$

$$= \Big\{\prod_{i=1}^{n-1} a_i\Big\}a_n \quad \text{(by definition and induction hypothesis)}$$

$$= \prod_{i=1}^{n} a_i \quad \text{(by definition).}$$

This computation is valid unless $n_{r-1} = n - 1$; the modification necessary in this case is left to the reader.

If all $a_i = a$, then $\prod_{i=1}^{n} a_i = a^n$, and (1) and (2) are consequences (for positive exponents) of the general associative law.

§ 2. Groups

DEFINITION. *A set G which is closed under a given multiplication is called a* GROUP *if the following conditions* (GROUP AXIOMS) *are satisfied*:

G_1. *The set G is not empty.*

G_2. *If $a, b, c \in G$, then $(ab)c = a(bc)$* (ASSOCIATIVE LAW).

G_3. *There exists in G an element e such that*

(1) *For any element a in G, $ea = a$.*

(2) *For any element a in G there exists an element a' in G such that $a'a = e$.*

In view of axiom G_2 and the general associativity law proved above, we can write the product of any (finite) member of elements of G without inserting parentheses.

We proceed to show that e is an identity in G, and that for every element a has an inverse. If a is given, then by G_3 (2), there exists an a' such that $a'a = e$, and there exists an a'' such that $a''a' = e$. Then $aa' = e(aa') = (a''a')(aa') = a''(a'a)a' = a''ea' = e$; this, together with $a'a = e$, shows that a' is an inverse of a, *provided* that e is an identity. But this is immediate, for $ea = a$ by G_3 (1), and $ae = a(a'a) = (aa')a = ea = a$.

Since e is an identity in G and a' an inverse of a, it follows that both are uniquely determined. As mentioned in the preceding section, the inverse of a will be denoted by a^{-1}.

If a and b are elements of a group G, then each of the equations $ax = b$, $xa = b$, has one and only one solution. Consider, for instance, the equation $ax = b$. Multiplication on the left by a^{-1} yields $x = a^{-1}b$ as the only possible solution, and direct substitution shows that $a^{-1}b$ is indeed a solution. Similarly it can be seen that $x = ba^{-1}$ is the only solution of the equation $xa = b$.

An immediate consequence of the uniqueness of the solution of each of the above equations is the (right or left) *cancellation law*: *if $ax = ax'$ or if $xa = x'a$, then $x = x'$.*

The solvability of both equations $ax = b$, $xa = b$ is equivalent, *in the presence of* G_1 *and* G_2, to axiom G_3. For if we assume the solvability of the foregoing equations and if we assume furthermore G_1 and G_2, then we can prove G_3 as follows:

We fix an element c in G and we denote by e a solution of the equation $xc = c$. If now a is any element of G, let b be a solution of the equation $cx = a$. We will have then $ea = e(cb) = (ec)b = cb = a$, which establishes G_3 (1). As to G_3 (2), it is an immediate consequence of the solvability of the equation $xa = e$.

In practice, when testing a given set G against the group axioms, it is sometimes the case that the solvability of the equations $ax = b$, $xa = b$ follows more or less directly from the nature of the given binary operation in G. The task of proving that G is a group can therefore sometimes be simplified by using the solvability condition just stated, rather than axiom G_3.

A group which contains only a finite number of elements is called a *finite group*. By the *order* of a finite group is meant the number of elements in the group.

It may happen that a group G consists entirely of elements of the form a^n, where a is a fixed element of G, and n is an arbitrary integer, $\geqq 0$. If this is the case, G is called a *cyclic* group, and the element a is said *to generate* G.

§ 3. Subgroups. Given two groups G and H, denote by $\cdot$ and $\circ$ the group operations in G and in H respectively. We say that H is a *subgroup* of G if (1) H is a subset of G and (2) $a \cdot b = a \circ b$ for any pair of elements a, b in H.

Let H be a subgroup of G and let e and e' be the identity elements of G and H respectively. We have $e' \cdot e' = e' \circ e' = e'$ and $e' \cdot e = e'$.

Hence $e' \cdot e' = e' \cdot e$, and therefore, by the cancellation law which holds in G, $e' = e$. We thus see that *the identity element of a group G belongs to any subgroup H of G* (and is necessarily also the identity of H).

If H is a subgroup of G we shall *not* use different symbols (such as and ∘) to denote the group operations in G and H respectively. Both operations will be denoted by the same symbol, say, $\cdot$ *or* ∘.

Given a group G and a *non-empty* subset H_0 of G, there is a very simple criterion for H_0 to be the set of elements of a subgroup of G. Namely, we have the following necessary and sufficient condition: *if* $a, b \in H_0$, *then* $ab^{-1} \in H_0$. This condition is obviously necessary. On the other hand, if this condition is satisfied, then we have in the first place that H_0 contains the identity e of G (if a is any element of the *non-empty* set H_0, then $e = a \cdot a^{-1} \in H_0$). It follows that if $a \in H_0$, then also $a^{-1} \in H_0 (a^{-1} = e \cdot a^{-1} \in H_0)$, and if $a, b \in H_0$, then $a \cdot b = a \cdot (b^{-1})^{-1} \in H_0$. Thus H_0 is indeed a group H with respect to the group operation in G, and this group H is a subgroup of G.

Let G be an arbitrary group and let H be a subgroup of G. If a is any element of G, we denote by Ha the set of elements of G which are of the form ha, $h \in H$, and we call this set *a right coset of H*. In a similar fashion, we can define *left cosets* aH of H. If multiplication in G is commutative (§ 1), then any right coset is also a left coset: Ha and aH are identical sets.

Let Ha and Hb be two right cosets of H in G, and suppose that these two cosets have an element c in common: $c = h_1 a = h_2 b$; $h_1, h_2 \in H$. Then $b = h_2^{-1} h_1 a$, and for any element h of H we have $hb = (hh_2^{-1}h_1)a \in Ha$ (since H is a subgroup of G and hence $hh_2^{-1}h_1 \in H$). Thus $Hb \subset Ha$; and similarly we can show that $Ha \subset Hb$. *Therefore* $Ha = Hb$.

It follows that two right cosets Ha and Hb are either *disjoint* (that is, have no elements in common) or *coincide*. A similar result holds for left cosets. Note that $a \in Ha$, for H contains the identity of G. Hence every element of G belongs to some right (or left) coset.

H is said to be a *normal* (or *invariant*) subgroup of G if $Ha = aH$ for every a in G. An equivalent property is the following: for every a in G and every h in H, the element $a^{-1}ha$ belongs to H.

Suppose now that G is a finite group of order n, and let m be the order of H. Every right coset Ha of H contains then precisely m elements (if $h_1, h_2 \in H$ and $h_1 \neq h_2$, then $h_1 a \neq h_2 a$). Since every element of G belongs to one and only one right coset, it follows that m must be a divisor of n and that n/m is the number of *right* cosets of H. We have therefore proved that *if G is a finite group, then the order m of any*

subgroup H of G divides the order n of G. The quotient n/m is called *the index* of H *in* G.

If a is an arbitrary element of a group G, the elements a^n, n any integer $\geqq 0$, clearly form a subgroup H of G. We call H *the cyclic subgroup generated by the element* a. If this subgroup H is finite, say of order m, then m is called *the order* of the element a; otherwise, a is said to be of *infinite order*.

Let a be an element of G, of finite order m. There exist then pairs of distinct integers n, n' such that $a^n = a^{n'}$ (otherwise the cyclic group generated by a would be infinite). From $a^n = a^{n'}$ follows $a^{n-n'} = 1$, whence there exist positive integers ν such that $a^\nu = 1$. Let μ be the smallest of these integers. Then $1, a, a^2, \cdots, a^{\mu-1}$ are distinct elements, while if n is any integer and if, say, $n = q\mu + n'$, $0 \leqq n' < \mu$, then

$$a^n = a^{q\mu+n'} = (a^\mu)^q \cdot a^{n'} = a^{n'}. \tag{1}$$

It follows that the cyclic group generated by a consists precisely of the μ elements $1, a, a^2, \cdots, a^{\mu-1}$, *and hence* $\mu = m$. Thus the order of a is also the smallest positive integer m such that $a^m = 1$.

From (1) it follows that $a^n = 1$ if and only if $n' = 0$, that is, if and only if n is a multiple of $m(= \mu)$.

It is clear that if G is a finite group, then every element a of G has finite order, and that the order of a divides the order of G.

§ 4. **Abelian groups.** Let G be a set with an associative multiplication. As defined in § 1, the multiplication is said to be commutative if $ab = ba$ for any elements a, b in G. In such a case it is permissible to change freely the order of the factors in a product $a_1 a_2 \cdots a_n$. That is to say, we have the general commutative law, which can be formally stated as follows:

Let φ be a permutation of the integers $\{1, 2, \cdots, n\}$. Then

$$\prod_{i=1}^{n} a_i = \prod_{i=1}^{n} a_{\varphi(i)}.$$

The proof is by induction and may be left to the reader.

A *group* G in which the group operation is commutative is said to be *commutative* or *abelian*. The group operation is then often written additively; that is, we write $a + b$ instead of ab and $\sum a_i$ instead of $\prod a_i$. The element $a + b$ is called the *sum* of a and b. The identity element is denoted by 0 (*zero*) and the inverse of a by $-a$. Correspondingly one writes na instead of a^n, and the rules for exponents take the form

$$ma + na = (m + n)a, \tag{1}$$

(2) $$m(na) = (mn)a,$$

(3) $$n(a + b) = na + nb,$$

(4) $$-(na) = (-n)a.$$

The last equation is a paraphrase of the statement (in the multiplicative notation) that the inverse of a^n is a^{-n}. The equation $xa = b$, which in the abelian case is equivalent to the equation $ax = b$, assumes then the form $x + a = b$. Its unique solution $b + (-a)$ is denoted by $b - a$ and is called *the difference of b and a*. The binary operation which associates with the ordered pair (a, b) the difference $b - a$ is called *subtraction*.

§ 5. Rings

DEFINITION. *A set R in which two binary operations,* $+$ *(addition) and* $\cdot$ *(multiplication), are given is called a* RING *if the following conditions* (RING AXIOMS) *are satisfied*:

R_1. *R is an abelian group with respect to addition.*

R_2. If $a, b, c \in R$, *then* $a(bc) = (ab)c$.

R_3. *If* $a, b, c \in R$, *then* $a(b + c) = ab + ac$ *and* $(b + c)a = ba + ca$ *(distributive laws).*

In conformity with the additive notation for abelian groups (§ 4) the identity element of R (regarded as an additive group) is denoted by 0, and the (additive) inverse of an element a is denoted by $-a$. Therefore the following relations hold in any ring R:

$$0 + a = a + 0 = a,$$
$$a + (-a) = (-a) + a = 0,$$
$$-(-a) = a,$$
$$a + (b + c) = (a + b) + c,$$
$$a + b = b + a.$$

The abelian group which, according to the ring axiom R_1, any ring R forms with respect to addition is called the *additive group of the ring*.

A ring R is called *commutative* if multiplication is commutative in R: $ab = ba$ for any elements a, b in R.

The distributive laws hold also for subtraction:

(1) $$a(b - c) = ab - ac; \qquad (b - c)a = ba - ca.$$

To prove, for instance, the first of these two relations, we have to show that $a(b - c) + ac = ab$. This, however, follows directly from the first distributive law R_3, since $(b - c) + c = b$.

For $b = c$, relations (1) yield the following important property of the element 0:

$$a0 = 0a = 0, \tag{2}$$

for all a in R. If we put in (1) $b = 0$ we find

$$a(-c) = -ac; \quad (-c)a = -ca,$$

and if in the first of these relations we replace a by $-a$ we obtain $(-a)(-c) = -(-a)c = -(-ac)$, whence

$$(-a)(-c) = ac. \tag{3}$$

An element a of R is called a *left* (or *right*) *zero divisor* if there exists in R an element b *different from zero* such that $ab = 0$ (or $ba = 0$). By (2) the element 0 is always both a left and right zero divisor whenever R contains elements different from zero. However, it is convenient to regard 0 as a zero divisor also in the trivial case of a ring R which consists only of the element zero (*nullring*). By a *proper* zero divisor is meant a zero divisor which is different from 0. Hence a ring R has proper zero divisors if and only if it is possible to have in R a relation $ab = 0$ *with both a and b different from zero.* In the sequel we shall call R *a ring without zero divisors* if R has no *proper* zero divisors. An element of R which is not a zero divisor will be called a *regular* element. In particular, the element 0 is not a regular element.

§ 6. **Rings with identity.** If there exists in the ring R an element which is an identity *with respect to multiplication*, then, by a remark made in § 1, this element is uniquely determined. *If R is not a nullring*, we shall refer to this element as the *identity* of the ring and we shall denote it by the symbol 1. In such a ring, multiplicative inverses are referred to simply as inverses. Hence an inverse of a is an element a' such that $a'a = 1$ and $aa' = 1$; it is unique according to § 1 and will be denoted by a^{-1}.

The element 1 is its own inverse. Similarly it follows from (3) that -1 is its own inverse.

The elements 0 and 1 are distinct elements of R. For we have agreed that R is not a nullring, and if $a \neq 0$, then $a0 = 0$ and $a1 = a \neq 0$, whence $0 \neq 1$. From this it follows that *the element 0 has no inverse*, since for any element a in R we have $a0 = 0a = 0 \neq 1$. *Consequently a ring* (which is not a nullring) *is definitely not a group with respect to multiplication.*

An element of R is called a *unit* if it has an inverse. The elements 1 and -1 are units. The ring of integers is the simplest example of a