Proof. Since the relation "a is conjugate to b" is an equivalence relation on G, the distinct conjugacy classes in G form a partition of G. Thus, $|G|$ is equal to the sum of the numbers of elements of the distinct conjugacy classes. There are $|C|$ conjugacy classes (corresponding to the elements of C) containing only one member, whereas $n_1, n_2, \ldots, n_k$ are the numbers of elements of the remaining conjugacy classes. This yields the class equation. To show that each n_i divides $|G|$, it suffices to note that n_i is the number of conjugates of some $a \in G$ and so equal to the number of left cosets of G modulo $N(\langle a \rangle)$ by Theorem 1.25. □

2. RINGS AND FIELDS

In most of the number systems used in elementary arithmetic there are two distinct binary operations: addition and multiplication. Examples are provided by the integers, the rational numbers, and the real numbers. We now define a type of algebraic structure known as a ring that shares some of the basic properties of these number systems.

1.28. Definition. A *ring* $(R, +, \cdot)$ is a set R, together with two binary operations, denoted by $+$ and $\cdot$, such that:

1. R is an abelian group with respect to $+$.
2. $\cdot$ is associative—that is, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$.
3. The *distributive laws* hold; that is, for all $a, b, c \in R$ we have $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$.

We shall use R as a designation for the ring $(R, +, \cdot)$ and stress that the operations $+$ and $\cdot$ are not necessarily the ordinary operations with numbers. In following convention, we use 0 (called the *zero element*) to denote the identity element of the abelian group R with respect to addition, and the additive inverse of a is denoted by $-a$; also, $a + (-b)$ is abbreviated by $a - b$. Instead of $a \cdot b$ we will usually write ab. As a consequence of the definition of a ring one obtains the general property $a0 = 0a = 0$ for all $a \in R$. This, in turn, implies $(-a)b = a(-b) = -ab$ for all $a, b \in R$.

The most natural example of a ring is perhaps the ring of ordinary integers. If we examine the properties of this ring, we realize that it has properties not enjoyed by rings in general. Thus, rings can be further classified according to the following definitions.

1.29. Definition

(i) A ring is called a *ring with identity* if the ring has a multiplicative identity—that is, if there is an element e such that $ae = ea = a$ for all $a \in R$.

(ii) A ring is called *commutative* if $\cdot$ is commutative.

(iii) A ring is called an *integral domain* if it is a commutative ring with identity $e \neq 0$ in which $ab = 0$ implies $a = 0$ or $b = 0$.
(iv) A ring is called a *division ring* (or *skew field*) if the nonzero elements of R form a group under $\cdot$.
(v) A commutative division ring is called a *field*.

Since our study is devoted to fields, we emphasize again the definition of this concept. In the first place, a *field* is a set F on which two binary operations, called addition and multiplication, are defined and which contains two distinguished elements 0 and e with $0 \neq e$. Furthermore, F is an abelian group with respect to addition having 0 as the identity element, and the elements of F that are $\neq 0$ form an abelian group with respect to multiplication having e as the identity element. The two operations of addition and multiplication are linked by the distributive law $a(b + c) = ab + ac$. The second distributive law $(b + c)a = ba + ca$ follows automatically from the commutativity of multiplication. The element 0 is called the *zero element* and e is called the *multiplicative identity element* or simply the *identity*. Later on, the identity will usually be denoted by 1.

The property appearing in Definition 1.29(iii)—namely, that $ab = 0$ implies $a = 0$ or $b = 0$—is expressed by saying that there are *no zero divisors*. In particular, a field has no zero divisors, for if $ab = 0$ and $a \neq 0$, then multiplication by a^{-1} yields $b = a^{-1}0 = 0$.

In order to give an indication of the generality of the concept of ring, we present some examples.

1.30. Examples

(i) Let R be any abelian group with group operation $+$. Define $ab = 0$ for all $a, b \in R$; then R is a ring.
(ii) The integers form an integral domain, but not a field.
(iii) The even integers form a commutative ring without identity.
(iv) The functions from the real numbers into the real numbers form a commutative ring with identity under the definitions for $f + g$ and fg given by $(f + g)(x) = f(x) + g(x)$ and $(fg)(x) = f(x)g(x)$ for $x \in \mathbf{R}$.
(v) The set of all 2×2 matrices with real numbers as entries forms a noncommutative ring with identity with respect to matrix addition and multiplication. □

We have seen above that a field is, in particular, an integral domain. The converse is not true in general (see Example 1.30(ii)), but it will hold if the structures contain only finitely many elements.

1.31. Theorem. *Every finite integral domain is a field.*

Proof. Let the elements of the finite integral domain R be $a_1, a_2, \ldots, a_n$. For a fixed nonzero element $a \in R$, consider the products $aa_1, aa_2, \ldots, aa_n$. These are distinct, for if $aa_i = aa_j$, then $a(a_i - a_j) = 0$, and

since $a \neq 0$ we must have $a_i - a_j = 0$, or $a_i = a_j$. Thus each element of R is of the form aa_i, in particular, $e = aa_i$ for some i with $1 \leqslant i \leqslant n$, where e is the identity of R. Since R is commutative, we have also $a_i a = e$, and so a_i is the multiplicative inverse of a. Thus the nonzero elements of R form a commutative group, and R is a field. □

1.32. Definition. A subset S of a ring R is called a *subring* of R provided S is closed under $+$ and $\cdot$ and forms a ring under these operations.

1.33. Definition. A subset J of a ring R is called an *ideal* provided J is a subring of R and for all $a \in J$ and $r \in R$ we have $ar \in J$ and $ra \in J$.

1.34. Examples

(i) Let R be the field $\mathbb{Q}$ of rational numbers. Then the set $\mathbb{Z}$ of integers is a subring of $\mathbb{Q}$, but not an ideal since, for example, $1 \in \mathbb{Z}$, $\frac{1}{2} \in \mathbb{Q}$, but $\frac{1}{2} \cdot 1 = \frac{1}{2} \notin \mathbb{Z}$.

(ii) Let R be a commutative ring, $a \in R$, and let $J = \{ra : r \in R\}$, then J is an ideal.

(iii) Let R be a commutative ring. Then the smallest ideal containing a given element $a \in R$ is the ideal $(a) = \{ra + na : r \in R, n \in \mathbb{Z}\}$. If R contains an identity, then $(a) = \{ra : r \in R\}$. □

1.35. Definition. Let R be a commutative ring. An ideal J of R is said to be *principal* if there is an $a \in R$ such that $J = (a)$. In this case, J is also called the principal ideal *generated by a.*

Since ideals are normal subgroups of the additive group of a ring, it follows immediately that an ideal J of the ring R defines a partition of R into disjoint cosets, called *residue classes* modulo J. The residue class of the element a of R modulo J will be denoted by $[a] = a + J$, since it consists of all elements of R that are of the form $a + c$ for some $c \in J$. Elements $a, b \in R$ are called *congruent* modulo J, written $a \equiv b \bmod J$, if they are in the same residue class modulo J, or equivalently, if $a - b \in J$ (compare with Definition 1.4). One can verify that $a \equiv b \bmod J$ implies $a + r \equiv b + r \bmod J$, $ar \equiv br \bmod J$, and $ra \equiv rb \bmod J$ for any $r \in R$ and $na \equiv nb \bmod J$ for any $n \in \mathbb{Z}$. If, in addition, $r \equiv s \bmod J$, then $a + r \equiv b + s \bmod J$ and $ar \equiv bs \bmod J$.

It is shown by a straightforward argument that the set of residue classes of a ring R modulo an ideal J forms a ring with respect to the operations

$$(a + J) + (b + J) = (a + b) + J, \tag{1.2}$$

$$(a + J)(b + J) = ab + J. \tag{1.3}$$

1.36. Definition. The ring of residue classes of the ring R modulo the ideal J under the operations (1.2) and (1.3) is called the *residue class ring* (or *factor ring*) of R modulo J and is denoted by R/J.

1.37. Example (The residue class ring $\mathbb{Z}/(n)$). As in the case of groups (compare with Definition 1.5), we denote the coset or residue class of the integer a modulo the positive integer n by $[a]$, as well as by $a+(n)$, where (n) is the principal ideal generated by n. The elements of $\mathbb{Z}/(n)$ are

$$[0]=0+(n),\ [1]=1+(n),\ldots,[n-1]=n-1+(n). \qquad \square$$

1.38. Theorem. *$\mathbb{Z}/(p)$, the ring of residue classes of the integers modulo the principal ideal generated by a prime p, is a field.*

Proof. By Theorem 1.31 it suffices to show that $\mathbb{Z}/(p)$ is an integral domain. Now $[1]$ is an identity of $\mathbb{Z}/(p)$, and $[a][b]=[ab]=[0]$ if and only if $ab=kp$ for some integer k. But since p is prime, p divides ab if and only if p divides at least one of the factors. Therefore, either $[a]=[0]$ or $[b]=[0]$, so that $\mathbb{Z}/(p)$ contains no zero divisors. $\square$

1.39. Example. Let $p=3$. Then $\mathbb{Z}/(p)$ consists of the elements [0], [1], and [2]. The operations in this field can be described by operation tables that are similar to Cayley tables for finite groups (see Example 1.7):

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

·	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

$\square$

The residue class fields $\mathbb{Z}/(p)$ are our first examples of *finite fields* —that is, of fields that contain only finitely many elements. The general theory of such fields will be developed later on.

The reader is cautioned not to assume that in the formation of residue class rings all the properties of the original ring will be preserved in all cases. For example, the lack of zero divisors is not always preserved, as may be seen by considering the ring $\mathbb{Z}/(n)$, where n is a composite integer.

There is an obvious extension from groups to rings of the definition of a homomorphism. A mapping $\varphi: R \to S$ from a ring R into a ring S is called a *homomorphism* if for any $a, b \in R$ we have

$$\varphi(a+b)=\varphi(a)+\varphi(b) \quad \text{and} \quad \varphi(ab)=\varphi(a)\varphi(b).$$

Thus a homomorphism $\varphi: R \to S$ preserves both operations + and · of R and induces a homomorphism of the additive group of R into the additive group of S. The set

$$\ker\varphi=\{a \in R: \varphi(a)=0 \in S\}$$

is called the *kernel* of φ. Other concepts, such as that of an *isomorphism*, are analogous to those in Definition 1.16. The homomorphism theorem for rings, similar to Theorem 1.23 for groups, runs as follows.

1.40. Theorem (Homomorphism Theorem for Rings). *If φ is a homomorphism of a ring R onto a ring S, then* $\ker\varphi$ *is an ideal of R and S is*

isomorphic to the factor ring $R/\ker\varphi$. Conversely, if J is an ideal of the ring R, then the mapping $\psi: R \to R/J$ defined by $\psi(a) = a + J$ for $a \in R$ is a homomorphism of R onto R/J with kernel J.

Mappings can be used to transfer a structure from an algebraic system to a set without structure. For instance, let R be a ring and let φ be a one-to-one and onto mapping from R to a set S; then by means of φ one can define a ring structure on S that converts φ into an isomorphism. In detail, let s_1 and s_2 be two elements of S and let r_1 and r_2 be the elements of R uniquely determined by $\varphi(r_1) = s_1$ and $\varphi(r_2) = s_2$. Then one defines $s_1 + s_2$ to be $\varphi(r_1 + r_2)$ and $s_1 s_2$ to be $\varphi(r_1 r_2)$, and all the desired properties are satisfied. This structure on S may be called the ring structure *induced by* φ. In case R has additional properties, such as being an integral domain or a field, then these properties are inherited by S. We use this principle in order to arrive at a more convenient representation for the finite fields $\mathbb{Z}/(p)$.

1.41. Definition. For a prime p, let $\mathbb{F}_p$ be the set $\{0, 1, \ldots, p-1\}$ of integers and let $\varphi: \mathbb{Z}/(p) \to \mathbb{F}_p$ be the mapping defined by $\varphi([a]) = a$ for $a = 0, 1, \ldots, p-1$. Then $\mathbb{F}_p$, endowed with the field structure induced by φ, is a finite field, called the *Galois field of order p*.

By what we have said before, the mapping $\varphi: \mathbb{Z}/(p) \to \mathbb{F}_p$ is then an isomorphism, so that $\varphi([a]+[b]) = \varphi([a]) + \varphi([b])$ and $\varphi([a][b]) = \varphi([a])\varphi([b])$. The finite field $\mathbb{F}_p$ has zero element 0, identity 1, and its structure is exactly the structure of $\mathbb{Z}/(p)$. Computing with elements of $\mathbb{F}_p$ therefore means ordinary arithmetic of integers with reduction modulo p.

1.42. Examples

(i) Consider $\mathbb{Z}/(5)$, isomorphic to $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$, with the isomorphism given by: $[0] \to 0$, $[1] \to 1$, $[2] \to 2$, $[3] \to 3$, $[4] \to 4$. The tables for the two operations $+$ and $\cdot$ for elements in $\mathbb{F}_5$ are as follows:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

(ii) An even simpler and more important example is the finite field $\mathbb{F}_2$. The elements of this field of order two are 0 and 1, and the operation tables have the following form:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

In this context, the elements 0 and 1 are called *binary elements*. □

If b is any nonzero element of the ring $\mathbb{Z}$ of integers, then the additive order of b is infinite; that is, $nb = 0$ implies $n = 0$. However, in the ring $\mathbb{Z}/(p)$, p prime, the additive order of every nonzero element b is p; that is, $pb = 0$, and p is the least positive integer for which this holds. It is of interest to formalize this property.

1.43. Definition. If R is an arbitrary ring and there exists a positive integer n such that $nr = 0$ for every $r \in R$, then the least such positive integer n is called the *characteristic* of R and R is said to have (positive) characteristic n. If no such positive integer n exists, R is said to have characteristic 0.

1.44. Theorem. *A ring $R \neq \{0\}$ of positive characteristic having an identity and no zero divisors must have prime characteristic.*

Proof. Since R contains nonzero elements, R has characteristic $n \geqslant 2$. If n were not prime, we could write $n = km$ with $k, m \in \mathbb{Z}$, $1 < k, m < n$. Then $0 = ne = (km)e = (ke)(me)$, and this implies that either $ke = 0$ or $me = 0$ since R has no zero divisors. It follows that either $kr = (ke)r = 0$ for all $r \in R$ or $mr = (me)r = 0$ for all $r \in R$, in contradiction to the definition of the characteristic n. □

1.45. Corollary. *A finite field has prime characteristic.*

Proof. By Theorem 1.44 it suffices to show that a finite field F has a positive characteristic. Consider the multiples $e, 2e, 3e, \ldots$ of the identity. Since F contains only finitely many distinct elements, there exist integers k and m with $1 \leqslant k < m$ such that $ke = me$, or $(m-k)e = 0$, and so F has a positive characteristic. □

The finite field $\mathbb{Z}/(p)$ (or, equivalently, $\mathbb{F}_p$) obviously has characteristic p, whereas the ring $\mathbb{Z}$ of integers and the field $\mathbb{Q}$ of rational numbers have characteristic 0. We note that in a ring R of characteristic 2 we have $2a = a + a = 0$, hence $a = -a$ for all $a \in R$. A useful property of commutative rings of prime characteristic is the following.

1.46. Theorem. *Let R be a commutative ring of prime characteristic p. Then*

$$(a+b)^{p^n} = a^{p^n} + b^{p^n} \quad \text{and} \quad (a-b)^{p^n} = a^{p^n} - b^{p^n}$$

for $a, b \in R$ and $n \in \mathbb{N}$.

Proof. We use the fact that

$$\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{1 \cdot 2 \cdot \cdots \cdot i} \equiv 0 \bmod p$$

for all $i \in \mathbb{Z}$ with $0 < i < p$, which follows from $\binom{p}{i}$ being an integer and the observation that the factor p in the numerator cannot be cancelled. Then by

the binomial theorem (see Exercise 1.8),

$$(a+b)^p = a^p + \binom{p}{1}a^{p-1}b + \cdots + \binom{p}{p-1}ab^{p-1} + b^p = a^p + b^p,$$

and induction on n completes the proof of the first identity. By what we have shown, we get

$$a^{p^n} = ((a-b)+b)^{p^n} = (a-b)^{p^n} + b^{p^n},$$

and the second identity follows. □

Next we will show for the case of commutative rings with identity which ideals give rise to factor rings that are integral domains or fields. For this we need some definitions from ring theory.

Let R be a commutative ring with identity. An element $a \in R$ is called a *divisor* of $b \in R$ if there exists $c \in R$ such that $ac = b$. A *unit* of R is a divisor of the identity; two elements $a, b \in R$ are said to be *associates* if there is a unit ε of R such that $a = b\varepsilon$. An element $c \in R$ is called a *prime element* if it is no unit and if it has only the units of R and the associates of c as divisors. An ideal $P \neq R$ of the ring R is called a *prime ideal* if for $a, b \in R$ we have $ab \in P$ only if either $a \in P$ or $b \in P$. An ideal $M \neq R$ of R is called a *maximal ideal* of R if for any ideal J of R the property $M \subseteq J$ implies $J = R$ or $J = M$. Furthermore, R is said to be a *principal ideal domain* if R is an integral domain and if every ideal J of R is principal—that is, if there is a generating element a for J such that $J = (a) = \{ra : r \in R\}$.

1.47. Theorem. *Let R be a commutative ring with identity. Then:*

(i) *An ideal M of R is a maximal ideal if and only if R/M is a field.*
(ii) *An ideal P of R is a prime ideal if and only if R/P is an integral domain.*
(iii) *Every maximal ideal of R is a prime ideal.*
(iv) *If R is a principal ideal domain, then $R/(c)$ is a field if and only if c is a prime element of R.*

Proof.

(i) Let M be a maximal ideal of R. Then for $a \notin M$, $a \in R$, the set $J = \{ar + m : r \in R, m \in M\}$ is an ideal of R properly containing M, and therefore $J = R$. In particular, $ar + m = 1$ for some suitable $r \in R$, $m \in M$, where 1 denotes the multiplicative identity element of R. In other words, if $a + M \neq 0 + M$ is an element of R/M different from the zero element in R/M, then it possesses a multiplicative inverse, because $(a + M)(r + M) = ar + M = (1 - m) + M = 1 + M$. Therefore, R/M is a field. Conversely, let R/M be a field and let $J \supseteq M$, $J \neq M$, be an ideal of R. Then for $a \in J$, $a \notin M$, the residue class $a + M$ has a multi-

plicative inverse, so that $(a + M)(r + M) = 1 + M$ for some $r \in R$. This implies $ar + m = 1$ for some $m \in M$. Since J is an ideal, we have $1 \in J$ and therefore $(1) = R \subseteq J$, hence $J = R$. Thus M is a maximal ideal of R.

(ii) Let P be a prime ideal of R; then R/P is a commutative ring with identity $1 + P \neq 0 + P$. Let $(a + P)(b + P) = 0 + P$, hence $ab \in P$. Since P is a prime ideal, either $a \in P$ or $b \in P$; that is, either $a + P = 0 + P$ or $b + P = 0 + P$. Thus, R/P has no zero divisors and is therefore an integral domain. The converse follows immediately by reversing the steps of this proof.

(iii) This follows from (i) and (ii) since every field is an integral domain.

(iv) Let $c \in R$. If c is a unit, then $(c) = R$ and the ring $R/(c)$ consists only of one element and is no field. If c is neither a unit nor a prime element, then c has a divisor $a \in R$ that is neither a unit nor an associate of c. We note that $a \neq 0$, for if $a = 0$, then $c = 0$ and a would be an associate of c. We can write $c = ab$ with $b \in R$. Next we claim that $a \notin (c)$. For otherwise $a = cd = abd$ for some $d \in R$, or $a(1 - bd) = 0$. Since $a \neq 0$, this would imply $bd = 1$, so that d would be a unit, which contradicts the fact that a is not an associate of c. It follows that $(c) \subseteq (a) \subseteq R$, where all containments are proper, and so $R/(c)$ cannot be a field because of (i). Finally, we are left with the case where c is a prime element. Then $(c) \neq R$ since c is no unit. Furthermore, if $J \supseteq (c)$ is an ideal of R, then $J = (a)$ for some $a \in R$ since R is a principal ideal domain. It follows that $c \in (a)$, and so a is a divisor of c. Consequently, a is either a unit or an associate of c, so that either $J = R$ or $J = (c)$. This shows that (c) is a maximal ideal of R. Hence $R/(c)$ is a field by (i). □

As an application of this theorem, let us consider the case $R = \mathbb{Z}$. We note that $\mathbb{Z}$ is a principal ideal domain since the additive subgroups of $\mathbb{Z}$ are already generated by a single element because of Theorem 1.15(i). A prime number p fits the definition of a prime element, and so Theorem 1.47(iv) yields another proof of the known result that $\mathbb{Z}/(p)$ is a field. Consequently, (p) is a maximal ideal and a prime ideal of $\mathbb{Z}$. For a composite integer n, the ideal (n) is not a prime ideal of $\mathbb{Z}$, and so $\mathbb{Z}/(n)$ is not even an integral domain. Other applications will follow in the next section when we consider residue class rings of polynomial rings over fields.

3. POLYNOMIALS

In elementary algebra one regards a polynomial as an expression of the form $a_0 + a_1x + \cdots + a_nx^n$. The a_i's are called coefficients and are usually