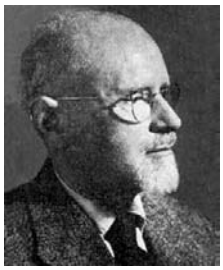
Algebra, Arithmetic and Geometry – With a View Toward Applications / 2005

Lectures : Tuesday/Thursday 18:15–19:15 ; LH-1, Department of Mathematics

3. Rings[1] — Prime rings

Remember that all our rings are rings with unity! Usually the term "rng" is used for a ring without unity. This term was suggested by LOUIS ROWEN and may be pronounced as "rŭng".



Adolf Abraham Halevi Fraenkel†
(1891-1965)

In the exercises below A denote a ring with unity 1_A (not necessarily commutative).

3.1. 1). Let a and b commuting elements in a ring A and let $n \in \mathbb{N}$. Then:

a). (Binomial Theorem) $(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i$.

b). (Polynomial formula) If $a_1, \ldots, a_r$ are pairwise commuting elements in a ring A, then for every $n \in \mathbb{N}$, we have the formula:

$$(a_1 + \cdots + a_r)^n = \sum_{\substack{(i_1,\ldots,i_r)\in\mathbb{N}^r \\ i_1+\cdots+i_r=n}} \frac{n!}{i_1! \cdots i_r!}\, a_1^{i_1} \cdots a_r^{i_r} .$$

c). $a^n - b^n = (a-b)(a^{n-1}+a^{n-2}b+\cdots+ab^{n-2}+b^{n-1}) = (a^{n-1}+a^{n-2}b+\cdots+ab^{n-2}+b^{n-1})(a-b)$. In particular, for every $a \in A$ and every $n \in \mathbb{N}^*$ we have:

$$a^n - 1 = (a-1)(a^{n-1} + \cdots + a + 1) = (a^{n-1} + \cdots + a + 1)(a-1) .$$

d). For every $a \in A$ and $n \in \mathbb{N}^*$, show that $(1-a)^2(1+2a+\cdots+na^{n-1}) = 1-(n+1)a^n+na^{n+1}$.

2). Prove the following well-known polarisation formula : For $n \in \mathbb{N}^*$ and arbitrary pariwise commuting elements $a_1, \ldots, a_n$ in a ring A, we have

$$2^{n-1} n!\, a_1 \cdots a_n = \sum_{\varepsilon} \varepsilon_2 \cdots \varepsilon_n (a_1 + \varepsilon_2 a_2 + \cdots + \varepsilon_n a_n)^n ,$$

where the right hand sum runs throught all sign-tuples $\varepsilon = (\varepsilon_2, \ldots, \varepsilon_n) \in \{1, -1\}^{n-1}$. (**Hint :** In the case $n = 2$ this is the formula $4a_1a_2 = (a_1+a_2)^2 - (a_1-a_2)^2$.)

In a similar way prove the following formula :

$$(-1)^n n!\, a_1 \cdots a_n = \sum_{H\subseteq\{1,\ldots,n\}} (-1)^{|H|} a_H^n = \sum_{e} (-1)^{e_1+\cdots+e_n} (e_1a_1 + \cdots + e_na_n)^n$$

where $a_H := \sum_{i\in H} a_i$ for $H \subseteq \{1, \ldots, n\}$) and the sum on the right side runs through all tuples $e = (e_1, \ldots, e_n) \in \{0\,,\ 1\}^n$. (**Remark :** This generalises the formula $2a_1a_2 = (a_1+a_2)^2 - a_1^2 - a_2^2$.)

---

[1] For the first time the axioms of rings appear to have been formulated by A. FRAENKEL in an article in *Journal für die angewandete Mathematik*, vol. 145 (1914). Before this the term "Zahlring" (=number ring or ring of numbers) had been used by HILBERT in "Die Theorie der algebraische Zahlkörper", *Jahresbericht der Deutschen Mathematiker Vereiningung*, vol. 4, (1897).

3.2. Let A be a ring.

1). Let B_i, $i \in I$, be a family of subrings of A. Then the intersection $\cap_{i\in I} B_i$ is again a subring of A.

2). (Center of a ring) The set of elements of A which commute with all elements of A is a commutative subring $\mathrm{Z}(A)$ of A; it is called the center of A.

3). For a family a_i, $i \in I$ of elements in A, the set $B := \{ b \in A \mid ba_i = a_i b \text{ for all } i \in I \}$ is a subring of A.

4). (Characteristic of a ring) The order of the unity 1_A of A in the additive group of A is called the characteristic of A and is denoted by $\mathrm{Char}\, A$. A natural number $n \in \mathbb{N}$ is the characteristic $\mathrm{Char}\, A$ of A if and only if it generates the kernel of the canonical ring homomorphism $\chi_A : \mathbb{Z} \to A$, $m \mapsto m \cdot 1_A$. (**Remarks:** (If $n = \mathrm{Char}\, A$ or a multiple of $\mathrm{Char}\, A$, then $na = 0$ for all $a \in A$; because $na = (n \cdot 1_A) \cdot a = 0 \cdot a = 0$. Note that the characteristic of A is determined by its prime ring. All subrings of a ring A have the same characteristic as that of A. The characteristics of $\mathbb{Z}$ and $\mathbb{Q}$ are 0. A ring A has characteristic 1 if and only if A is a zero ring. In the power-set ring $\mathfrak{P}(X)$ (see Exerxise T3.2-2)) we have $2 \cdot 1_{\mathfrak{P}(X)} = X + X = (X \cup X) \smallsetminus (X \cap X) = \emptyset$, therefore, if $X \neq \emptyset$ then $\mathfrak{P}(X) = 2$.)

5). Let A be a ring of characteristic p, where p is a prime number. For two commuting elements $a, b \in A$ and every $n \in \mathbb{N}$, show that $(a+b)^{p^n} = a^{p^n} + b^{p^n}$. (**Hint:** Use binomial theorem (see Exercise 3.1-1)) and show that p divides the binomial coefficients $\binom{p}{i}$, $1 \leq i \leq p-1$.)

6). For $n \in \mathbb{N}^*$, let Z_n be a (additively written) cyclic groups of order n. If $N \subseteq \mathbb{N}^*$ is an infinite set of positive natural numbers, then there is no ring (with unity), whose additive group is the direct sum $\bigoplus_{n\in N} Z_n$.

3.3. (Unit group of a ring) The group of the invertible elements of the multiplicative monoid of A is called the unit group of A and is denoted by $A^\times$. Its elements are called the units of A. (**Remarks:** The units of $\mathbb{Z}$ are the numbers 1 and -1. In every ring A, 1 and -1 are units, since $1 = 1 \cdot 1 = (-1)(-1)$. The elements 1 and -1 in A need not be distinct: In fact $1_A = -1_A$ if and only if $2 \cdot 1_A = 0$, i.e. if $\mathrm{Char}\, A = 2$ or $\mathrm{Char}\, A = 1$. In particular, this is the sitiuation for the power-set ring $\mathfrak{P}(X)$ of a set X. In this ring the unit element $1_{\mathfrak{P}(X)} = X$ is the only unit.)

1). Let A_i, $i \in I$, be a family of rings. An element $(a_i)_{i\in I}$ of the direct product $B := \prod_{i\in I} A_i$ is a unit if and only if $a_i \in A_i^\times$ for all $i \in I$. Therefore $B^\times = \prod_{i\in I} A_i^\times$.

2). Let B is a subring of a ring A. Then $B^\times$ is a subgroup of $A^\times$. In particular, $B^\times \subseteq B \cap A^\times$. (**Remark:** In general $B^\times \neq B \cap A^\times$. For example, $\mathbb{Z} \cap \mathbb{Q}^\times = \mathbb{Z} \cap (\mathbb{Q} \smallsetminus \{0\}) = \mathbb{Z} \smallsetminus \{0\}$, but $\mathbb{Z}^\times = \{1, -1\}$.)

3). For the center of a ring we have: $\mathrm{Z}(A)^\times = \mathrm{Z}(A) \cap A^\times$. (**Hint:** If $a \in A^\times$ and $b \in A$ commute, then a^{-1} and b also commute.) (**Remark:** In general $\mathrm{Z}(A)^\times \neq \mathrm{Z}(A^\times) = \{a \in A^\times \mid ab = ba \text{ for all } b \in A^\times\}$.)

4). Let $a, b \in A$, where b is a unit in A which belongs to the center of A. Then $ab^{-1} = b^{-1}a$. This element is frequently written as — like a rational number— as a fraction: $a/b := \frac{a}{b} := ab^{-1} = b^{-1}a$.

(Finite geometric series) Let A be a commutative ring and $a, b \in A$ elements of A such that $a - b$ is a unit in A. For every $n \in \mathbb{N}^*$, we have $a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1} = \dfrac{a^n - b^n}{a-b}$.

In the special case, if $a \in A$ and $a - 1$ is a unit in A, then for every $n \in \mathbb{N}^*$ we have

$$a^{n-1} + \cdots + a + 1 = \frac{a^n - 1}{a - 1}.$$

5). (Rules of calculation for fractions) Let a, b, c, d be elements of a ring A, where b, d are units in A and belong to the center of A. Then:

(i) $\dfrac{a}{b} + \dfrac{c}{d} = \dfrac{ad + bc}{bd}$. (ii) $\dfrac{a}{b} \cdot \dfrac{c}{d} = \dfrac{ac}{bd}$. (iii) $\dfrac{a}{b} = \dfrac{ad}{bd}$. (iv) $\left(\dfrac{b}{d}\right)^{-1} = \dfrac{d}{b}$.

(v) $\dfrac{a}{b} = \dfrac{c}{d}$ if and only if $ad = bc$.

6). Let A be a ring with Char $A \neq 1, \neq 2$. If the unit group $A^\times$ of A is cyclic, then $A^\times$ is finite and $|A^\times|$ is an even number.

3.4. (Zero divisors and Non-zero divisors) An element a is called a left zero divisor (resp. right zero divisor) in A, if there exists a $b \in A$, $b \neq 0$, such that $ab = 0$ (resp. if there exists a $c \in A$, $c \neq 0$, such that $ca = 0$.) We say that a is a zero divisor, if a is either a left– or a right zero divisor in A; otherwise a is called a non-zero divisor in A. The set of non-zero divisors in A is denoted by A^*. (**Remarks:** In a commutative ring the three concepts of zero divisors are the same. If A is not a zero ring, then $0 \in A$ is a zero divisor in A. The unit element 1_A of A is a non-zero divisor in A.)

1). Let a, b be elements in a ring A. Then:

a). If a is a unit in A, then a is a non-zero divisor in A. In particular, $A^\times \subseteq A^*$.

b). If a, b are not left zero divisors (resp. not right zero divisors) in A, then ab is also not a left zero divisor (resp. not a right zero divisor) in A. In particular, $(A^*, \cdot)$ is a cancellative (see Exercise T3.1-7)) submonoid of the multiplicative monoid $(A, \cdot)$ of A.

c). The left translation $\lambda_a : A \to A$, $x \mapsto ax$ (resp. the right translation $\rho_a : A \to A$, $x \mapsto xa$) is injective if and only if a is not a left zero divisor (resp. not a right zero divisor) in A.

2). Let a be an element in a ring A.

a). If a has a left inverse a' and has a right inverse a'', then a is a unit and $a' = a^{-1} = a''$ (see Exercise T3.1-6)-b)).

b). Show that the following statements are equivalent:

(i) a is a unit. (ii) a has a left inverse and it is not a right zero divisor. (ii′) a has a right inverse and it is not a left zero divisor. (iii) a has exactly one left inverse. (iii′) a has exactly one right inverse. (iv) The right translation $\rho_a : A \to A$, $x \mapsto xa$ is bijective.

(iv′) The left translation $\lambda_a : A \to A$, $x \mapsto ax$ is bijective.

3.5. (Integral domains and fields) A ring A is said to be free from zero divisors if every non-zero element in A is a non-zero divisor. A ring A is called a domain if $A \neq 0$ and it is free from zero divisors, or equivalently if $A^* = A \setminus \{0\}$. A commutaive domain is called an integral domain.

A rings A is called a division ring or a skew-field if $A \neq 0$ and if every $a \in A$, $a \neq 0$ is a unit in A, or equivaletly if $A^\times = A \setminus \{0\}$, i.e., if set of all non-zero elements of A form a group under the ring multiplication of A. A commutative division ring is called a field.

1). Let A be a ring which is free from zero divisors. Then the following cancellation laws hold in A:

If $a \in A$, $a \neq 0$ and if $x, y \in A$ are arbitrary, then $ax = ay$ (resp. $xa = ya$) implies the equality $x = y$. In particular, if A is a domain, then $(A \setminus \{0\}, \cdot)$ is a monoid with cancellation law. — $\mathbb{Z}$ is an integral domain.

2). Subrings of a ring which is free from zero divisors (resp. domain, integral domain) are also rings which are free from zero divisors, (resp. domains, integral domains). If a subring K of a ring A is a division ring (resp. field), we say that K is a subdivision ring (resp. subfield) of A. The intersection of a non-empty family K_i, $i \in I$ of subdivision rings (resp. subfields) of a ring A is again a subdivision ring (resp. subfield) of A. The center $\mathrm{Z}(D)$ of a division ring D is a subfield of D.

3). The characteristic of a ring which is free from zero divisors is either 0, or 1, or a prime number. In particular, if A is a domain (resp. a division ring), then the characteristic of A is either 0 or a prime number.

4). (Quotient field) Let K be a field and let A be a subring of K. Then A is an integral domain. The smallest subfield Q of K which contain A; this is well-defined and exists, since it is the intersection of all subfields of K which contain A, in fact, it is $\mathrm{Q} = \{a/b \mid a, b \in A, b \neq 0\}$. This

subfield Q of K is called the quotient field of A in K (see Exercise 3.5-2)). If $Q = K$, then K is called the quotient field of A. for example, $\mathbb{Q}$ is the quotient field of $\mathbb{Z}$ in $\mathbb{Q}$, or in $\mathbb{R}$, or in $\mathbb{C}$, or more generally in any field K of charateristic 0.

Construction of the quotient field $Q(A)$ of an integral domain A : On the set $A \times (A \setminus \{0\})$ the relation $\sim$ defined by $(a, b) \sim (c, d)$ if $ad = bc$ is an equivalence relation; its equivalence classes are denoted by *fractions* a/b. then the addition and multiplication : $a/b + c/d := (ad + bc)/bd$ and $a/b)\cdot(c/d) := (ac)/(bd)$, $a, b, c, d \in A$, $b \neq 0, d \neq 0$, resp. are well-defined binary operations on the quotient set $Q(A) := A \times (A \setminus \{0\})/\sim$. With thgese definitions $(Q(A), +, \cdot)$ is a coomutative ring with unity $1/1$, moreover, a field and the map $A \to A \times (A \setminus \{0\}) \to Q(A)$ defined by $a \mapsto (a, 1) \mapsto a/1$ is an injective ring homomorphism. Therefore via this natural injective ring homomorphism A can be identified with a subring of $Q(A)$. Moreover, $Q(A)$ is the quotient field of A and every field K which conatin A, also contain $Q(A)$. In particular, $Q(A)$ is the smallest field containing A.

Let D be a divison ring and let A be a commutative subring of D. Then D contains a subfield which contains A. In particular, D contains a quotient field of A.

5). Let $Q(A)$ be the quotient field of the integral domain A. Then $\mathrm{card}(Q(A)) = \mathrm{card}(A)$. (**Hint :** For an infinite set X, $\mathrm{card}(X \times X) = \mathrm{card}(X)$ —this can be easily proved by using Zorn's lemma.)

6). (Vieta's root theorem) Let A be an integral domain and let $a_1, a_2 \in A$ two distinct elements and $b, c \in A$. Suppose that $a_1^2 + ba_1 + c = 0$ and $a_2^2 + ba_2 + c = 0$. Then show that $b = -(a_1 + a_2)$ and $c = a_1a_2$. Deduce that : for given elements $b, c \in A$, there are at most two elements $a \in A$ such that $a^2 + ba + c = 0$. (**Remark :** In general this assertion is true only if A is commutative. For example in the division rings of quaternion there are infinitely many elements a sith $a^2 + 1 = 0$.)

7). Let A be a finite commutative ring. Then

a). Show that every non-zero divisor is a unit. In particular, a non-zero domain is a divison ring.

(**Remark :** A famous theorem of Wedderburn states that : *every finite division ring is commutative and hence a field.*)

b). Let a be the product of all non-zero elements of A. Show that :

$$a = \begin{cases} -1, & \text{if } A \text{ is a field ;} \\ 2, & \text{if } A \text{ is a prime ring with 4 elements ;} \\ 0, & \text{otherwise .} \end{cases}$$

(**Hint :** Use the Exercise T3.1-9)-g) and the part a).)

3.6. (Nilpotent, Unipotent and Idempotent elements) Let a, b, e, u, v be elements in a ring A.

1). An element a of a ring A is called nilpotent, if there exists a natural number $m \in \mathbb{N}$ such that $a^m = 0$. Show that :

a). If a is nilpotent and if a and b commute, then ab is nilpotent.

b). If a and b are nilpotent and if a and b commute, then $a + b$ is nilpotent.

c). If a is nilpotent and e is a unit und if a and e commute, then $e - a$ is a unit.

2). An element u of a ring A is called unipotent, if $1 - u$ is nilpotent. Show that :

a). If u is unipotent, then u is a unit in A, i.e. $u \in A^\times$. Moreover, u^{-1} is also unipotent.

b). If $u, v \in A$ are unipotent and commute, then uv is also unipotent.

c). If A is commutative, then the set of unipotent elements in A is a subgroup of the unit group $A^\times$ of A.

3). Let A be a ring of characteristic p^n, where p is a prime number. An element $u \in A$ is unipotent if and only if u is a unit in A and the order of u in $A^\times$ is a power of p. If A has no non-zero nilpotent elements and if $a \in A^\times$ is an element of finite order, then $\gcd(p, \mathrm{Ord}\, a) = 1$.

4). An element a of a ring A is called idempotent, if $a^2 = a$.

a). If $a \in A$ is idempotent, then $a^n = a$ for all $n \in \mathbb{N}^*$. The elements 0 and 1 are clearly idempotent; they are called the trivial idempotent elements. Non-trivial idempotent elements are clearly zero divisors, since $a^2 = a$ and $a(1-a) = 0$ are equivalent.

b). In an integral domain 0 and 1 are the only idempotent elements.

c). If $a \in A$ is idempotent, then so is $1-a$. Two idempotent elements a, b of A with $a+b = 1$ are called complementary.

d). Let A_i, $i \in I$, be a family of rings with the identity elements $1_i \in A_i$ and the zero elements $0_i \in A_i$. In the product ring $B := \prod_{i\in I} A_i$, an element $(a_i)_{i\in I}$ is idempotent if and only if all a_i are idempotent in A_i. In particular, $e_j := (a_{ij})_{i\in I}$, where a_{ij} are defined by $a_{ij} := 0_i$ for $i \neq j$ and $a_{jj} := 1_j$, are idempotent elements in B, which are contained in the centre of B. If none of A_i is a zero ring then all e_j, $j \in I$, are distinct; further if $|I| \geq 2$ then none of them is 0 or 1, therefore they are non-trivial idempotent elements.

e). (Boolean rings) A ring A in which every element is idempotent, is called a Boolean ring. Let A be a non-zero Boolean ring. Then Char $A = 2$. Moreover, A commutative and $A^\times = \{1_A\}$. In the power-set ring $\mathfrak{P}(X)$ (see Exercise T3.2-2)) of any set X, every element is idempotent, and so the ring $\mathfrak{P}(X)$ and every subring of $\mathfrak{P}(X)$ is a Boolean ring. (**Remark:** Every Boolean ring is a subring of $\mathfrak{P}(X)$.)

f). Let a, b be idempotent elements in a ring A. Then:

(i) $a+b$ is idempotent if and only if $ab = ba$ and $2ab = 0$. Further, $a-b$ idempotent if and only if $ab = ba$ and $2(1-a)b = 0$.

(ii) If $ab = ba$, then ab, $a+b-ab$ and $(a-b)^2 = a+b-2ab$ are idempotent.

(iii) If $ab = ba$ and $a-b$ nilpotent, then $a = b$.

g). Let A be a commutative ring and $\mathrm{Idp}(A)$ be the set of all idempotent elements in A. Then $(\mathrm{Idp}(A), \triangle, \cdot)$ is a Boolean ring, with the addition $a \triangle b := (a-b)^2$ and the multiplication induced from the multiplication from A. Moreover, the rings $(\mathrm{Idp}(A), \triangle, \cdot)$ and $(A, +, \cdot)$ are equal if and only if A is a Boolean ring.

3.7. (Involutions) An element a in a (multiplicatively written) monoid is called involutory or an involution, if a^2 is equal to the identity element of the monoid. The involutory elements are precisely those invertible elements with self inverses. If the monoid is commutative, then the involutory elements form a subgroup of the group of the invertible elements. The product of two involutory elements is involutory if and only if these elements commute.

Let A be a ring and let $\mathrm{Inv}(A)$ denote the set of all (with respect to the multiplication of A) involutory elements, $\mathrm{Idp}(A)$ be the set of all idempotent elements of A. Then the map

$$\gamma : \mathrm{Idp}(A) \to \mathrm{Inv}(A),\ a \mapsto 1 - 2a$$

is injective, if $2 \cdot 1_A$ is a non-zero divisor in A and is bijective, if $2 \cdot 1_A$ is a unit in A. (If A is commutative, then γ is a group homomorphism of the additive group $\mathrm{Idp}(A)$ (see Exercise 3.6-4)-g)), into the multiplicative group $\mathrm{Inv}(A)$.)

3.8. Let A be a ring and let α, $\alpha' : A \to A$ be the maps defined by $\alpha(x) := x - x^2$, $\alpha'(x) := 1 - 2x$ respectively. If $\alpha(x)$ is nilpotent, then $(\alpha'(x))^2$ is unipotent and in particular, $\alpha'(x)$ is a unit in A.

Let $a \in A$ be such that $\alpha(a)$ is nilpotent. Then there exist unique elements $s, t \in A$ with the following properties: (i) $a = s + t$. (ii) s is idempotent and t is nilpotent. (iii) s and t commute. Moreover, these uniquely determined elements s and t belong to the smallest subring A' of A containing a. (Note that if $a = s + t$ is an element of A and s, $t \in A$ satisfy the conditions (ii) and (iii), then $\alpha(a)$ must be nilpotent.) (**Hint:** *Existence*: The recursively defined sequence a_i, $i \in \mathbb{N}$, with $a_0 := a$ and $a_{i+1} := a_i - \frac{\alpha(a_i)}{\alpha'(a_i)} = -\frac{a_i^2}{1-2a_i}$ is well-defined. Then $a_i \in A'$, $a_i = a + c_i\alpha(a)$ and $\alpha(a_i) = d_i(\alpha(a))^{2^i}$ with c_i, $d_i \in A'$. Now take $s := a_i$ with large i. —This process remind the *Newton's process* to construct a zero s

of the function α by approximating zeros of real differentiable functions. *Uniqueness*: The above construction show that to arbitrary decomposition $a = s + t$, where s and t satisfy the conditions (ii) and (iii), one can apply Exercise 3.6-4)-f) and conclude that s and t are unique.)

3.9. (Ring of numerical functions) Let A be a commutative ring. On the set of sequences $A^{\mathbb{N}^*}$ let the addition be defined componentwise by $(f+g)(n) := f(n) + g(n)$, $f, g \in A^{\mathbb{N}^*}$, $n \in \mathbb{N}^*$. Further, let the multiplication be defined by the formula:

$$(f * g)(n) := \sum_{d|n} f(d) g\Big(\frac{n}{d}\Big) .$$

(This binary operation is called the (Dirichlet's) convolution on $A^{\mathbb{N}^*}$. The elements of $A^{\mathbb{N}^*}$ are called numerical functions with values in in A.)

a). $\mathrm{ZF}(A) := (A^{\mathbb{N}^*}, +, *)$ is a commutative ring. (This ring is called the ring of numerical functions with values in A.) The unity (multiplicative identity) of this ring is the function ε, where $\varepsilon(1) := 1$ and $\varepsilon(n) := 0$ for $n \geq 2$. An element e of $\mathrm{ZF}(A)$ is a unit if and only if $e(1)$ a unit in A. (e^{-1} can be recursively determined by e.)

b). A numerical function $f \in \mathrm{ZF}(A)$ is called multiplicative, if $f(1) = 1$ and $f(mn) = f(m)f(n)$ for all $m, n \in \mathbb{N}^*$ with $\gcd(m, n) = 1$. If $f \in \mathrm{ZF}(A)$ is multiplicative and $g \in \mathrm{ZF}(A)$ is arbitrary, then $f * g$ is multiplicative if and only if g is multiplicative. The unit-element ε is multiplicative. In particular, the set of multiplicative numerical functions in $\mathrm{ZF}(A)$ is a subgroup of the unit group of $\mathrm{ZF}(A)$.

c). Let $\zeta \in \mathrm{ZF}(A)$ be the numerical function defined by $\zeta(n) = 1$ for all $n \in \mathbb{N}^*$. Then ζ is multiplicative and for $f \in \mathrm{ZF}(A)$ the function $\zeta * f$ is called the Summator-function of f, since $(\zeta * f)(n) = \sum_{d|n} f(d)$. Therefore (see b) above) f is multiplicative if and only if $\zeta * f$ is multiplicative. Further, in this case f can be recovered from $\zeta * f$ through the following inversion formula:

$$f(n) = \prod_{p \text{ prime},\, p|n} ((\zeta * f)(p^{\mathrm{v}_p(n)}) - (\zeta * f)(p^{\mathrm{v}_p(n)-1})) .$$

d). In the special case $A = \mathbb{Z}$, in addition to the numerical functions ε and ζ, the important Euler's φ-function φ, is a multiplicative numerical function. Further, the numerical function $\psi : n \mapsto n$ is multiplicative and $\zeta * \varphi = \psi$. Let $\mathrm{T}(n)$ (respectively $\mathrm{S}(n)$) denote the number of (respectively the sum of) positive integer-divisors of $n \in \mathbb{N}^*$. Then the numerical functions T and S are also multiplicative. (This can be deduced from the following identities: $\zeta * \zeta = \mathrm{T}$, $\zeta * \psi = \mathrm{S}$.)

e). (Möbius inverson formula) Let A be an arbitrary commutative ring. The numerical function $\mu := \zeta^{-1}$ is called the Möbius function. Then

$$f(n) = \sum_{d|n} \mu\Big(\frac{n}{d}\Big) \cdot (\zeta * f)(d) \qquad \text{for every } f \in \mathrm{ZF}(A) .$$

(This is immediate from $f = \mu * (\zeta * f)$. Using this formula and c) one can show easily that: $\mu(1) = 1$, $\mu(n) = (-1)^r$, if n is a product of distinct prime numbers and $\mu(n) = 0$ otherwise.)

f). The ring $\mathrm{ZF}(A)$ is an integral domain if and only if A is an integral domain.

3.10. (Prime rings) The subset $\mathbb{Z} \cdot 1_A := \{n \cdot 1_A \mid n \in \mathbb{Z}\}$ of a ring A is the smallest subring of A. This ring is called the prime ring of A. The prime ring of a ring A, is also the prime ring of each of its subring. The prime ring of $\mathbb{Z}$ is itself. In particular, $\mathbb{Z}$ has no other subring than itself. A ring which is its prime ring is called a prime ring. In particular, every prime ring is commutative and has proper subrings. Moreover, a ring A is a prime ring if and only if its additive group is cyclic.

1). (Structure of prime rings) Let A be a prim ring of the characteristic m.

(i) If $m > 0$, then $|A| = m$ and $A = \{n \cdot 1_A \mid 0 \leq n < m\}$. Two elements $r \cdot 1_A$, $s \cdot 1_A \in A$ with $r, s \in \mathbb{Z}$ are equal if and only if $r \equiv s$ modulo m. An element $r \cdot 1_A \in A$ with $r \in \mathbb{Z}$ is a non-zero divisor if and only if it is a unit; more over, equivalently $\mathrm{ggT}(r, m) = 1$.

(ii) If $m = 0$, then $A = \{n \cdot 1_A \mid n \in \mathbb{Z}\}$, where the elements $n \cdot 1_A$ are distinct for distinct inetegers $n \in \mathbb{Z}$ and so A is an integral domain with exactly two units 1_A and -1_A.

(**Remark:** By the above theorem all prime rings of charateristic $m \in \mathbb{N}$ have the same structure. In fact, if A is a prime ring of characteristic $m \in \mathbb{N}$, then the map $A \to \mathbb{Z}/\mathbb{Z}m$ defined by $r \cdot 1_A \mapsto [r]$ = the residue class of

r modulo m, is well-defined and is an isomorphism of rings. Therefore for concrete calculation in prime ring, we may choose the prime ring $A_m = \mathbb{Z}/\mathbb{Z}m$, $m \in \mathbb{N}$. In particular, $A_0 = \mathbb{Z}$.)

2). For a prime ring of charateristic $m > 0$, the following statements are equivalent:

(i) A is a field. (ii) A is an integral domain. (iii) m is a prime number.

3). Let A be a prime ring of charateristic $m > 0$. Then the order of the unit group $A^\times$ is $\varphi(m)$, where φ is the Euler's totient function. Deduce that:

a). (Euler's theorem) For $m \in \mathbb{N}^*$ and $r \in \mathbb{Z}$ with $\gcd(r, m) = 1$, we have $r^{\varphi(m)} \equiv 1 \bmod m$.

b). (Fermat's Little theorem) Let p be a prime number and let $r \in \mathbb{Z}$ which is not divisible by p. Then $r^{p-1} \equiv 1 \bmod p$. (**Hint:** *Proof-variant*: Since $\mathbb{Z}_p$ is an integral domain, it is enough to prove that $r^p \equiv r \bmod p$. For this it is enough to prove that: for every element a in a prime ring of charateristic p, we have $a^p = a$. Therefore let $a = s \cdot 1$ for some $s \in \mathbb{N}$ and hence by Exercise ??? we have $a^p = \left(\sum_{i=1}^{s} 1\right)^p = \sum_{i=1}^{s} 1^p = \sum_{i=1}^{s} 1 = a$.)

3.11. In the following exercises let A_m denote a prime ring of characteristic $m \in \mathbb{N}$, for example $\mathrm{A}_m = \mathbb{Z}/\mathbb{Z}m$.

1). a). A Mersenne number $2^p - 1$ with p prime and $p > 2$ can have only prime divisors of the form $2np + 1$ with $n \in \mathbb{N}^*$. (**Hint:** If q is a prime divisor of $2^p - 1$, p prime, then the order of $2 \cdot 1_{\mathrm{A}_q}$ in the unit group of A_q is equal to p.)

b). Every two distinct Mersenne numbers are relatively prime.

2). A Fermat-number $2^{2^t} + 1$ with $t \in \mathbb{N}$ can have only prime divisors of the form $n2^{t+1} + 1$ with $n \in \mathbb{N}^*$. (**Hint:** Use a method of proof as in 1).

3). Let A be a ring of characteristic $m > 0$. For an integer r, the following statements are equivalent:

(i) $r \cdot 1_A$ is a unit in A. (ii) $r \cdot 1_A$ is a unit in the prime ring of A. (iii) $\gcd(r, m) = 1$.

4). Let $m_1, \ldots, m_r$ be non-zero pairwise relatively prime natural numbers and $m := m_1 \cdots m_r$. Then $A := \prod_{i=1}^{r} \mathrm{A}_{m_i}$ is a prime ring of the characteristic m (see Exercise 3.10-1)). The unit group of A is the direct product of the unit groups of the prime rings A_{m_i}. What can you now conclude for the Euler's φ-function?

5). Let $m \in \mathbb{N}^*$, and let $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$ be the (normalised) prime factorisation of m.

a). For $s \in \mathbb{Z}$ the following statements are equivalent:

(i) $s \cdot 1_{\mathrm{A}_m}$ is nilpotent in A_m. (ii) s is a multiple of $p_1 \cdots p_r$.

b). A_m has exactly 2^r idempotent elements. (**Hint:** The natural numbers e with $0 \le e < m$ and $e \equiv e^2 \bmod m$ can be calculated (by using exercise 4)) in the direct product of prime rings of characteristic p^{α_i}, $i = 1, \ldots, r$ and hence one can reduce the problem to the case $r = 1$.)

6). Let p be a prime number ≥ 3.

a). In the unit group $\mathrm{A}_p^\times$, the element -1 is the only element of order 2.

b). (Wilson's Theorem) $(p-1)! \equiv -1 \bmod p$. (**Hint:** Apply ??? to the prime ring A_p.)

c). (Euler's criterion for the quadartic residues) Let $a \in \mathbb{Z}$ be not divisible by p. If there exists $b \in \mathbb{Z}$ with $b^2 \equiv a \bmod p$, then $a^{(p-1)/2} \equiv 1 \bmod p$. Further, if there is no $b \in \mathbb{Z}$ with $b^2 \equiv a \bmod p$, then $a^{(p-1)/2} \equiv -1 \bmod p$. (**Hint:** Apply Exercise 3.1-9)-g)-(ii) to the group $\mathrm{A}_p^\times$.)

d). If $p \equiv 1 \bmod 4$, then $\left(\left(\frac{p-1}{2}\right)!\right)^2 \equiv -1 \bmod p$ and if $p \equiv 3 \bmod 4$, then there exists no $b \in \mathbb{Z}$ with $b^2 \equiv -1 \bmod p$.

e). (Converse of the Wilson's theorem) If $n \in \mathbb{N}$, $n > 1$, and if $(n-1)! \equiv -1 \bmod n$, then n is a prime number. (**Hint:** Apply Exercise 3.5-7)-b) to the ring A_p. **Another Proof** (Pranesachar): Note that either if n has two distinct prime factors p and q or if n has a square factor p^2 with p odd prime, then n divides $(n-1)!$. In the remaining case $n = 2^2 = 4$ and $(n-1)! \bmod n = 3! \equiv \bmod 4 \equiv 2 \bmod 4 \not\equiv 1 \bmod 4$.)

(**Remark :** We can use the above exercise to give a proof of the two square theorem : *Every prime number* p . The solution of the congruence $b^2 + 1 \equiv 0 \bmod p$ for a prime number $p \equiv 1 \bmod 4$ gives the solution of the equation $c^2 + d^2 = p$ with $c,\ d \in \mathbb{N}^*$.)

7). Let $m, n \in \mathbb{N}^*$ and $m \geq 2$. Then show that n divides $\varphi(m^n - 1)$ and $2n$ divides $\varphi(m^n + 1)$.

(**Hint :** Compute the order of m in the prime rings A_{m^n-1} and A_{m^n+1} .)

Below one can see definitions and (simple) test-exercises.

Definitions and Test-Exercises

T3.1. (Monoids and Groups) Let $(M, \cdot)$ be a monoid with *neutral element* e , i.e. $e \cdot a = a \cdot e = a$ for every $a \in M$. (This neutral element is uniquely determined : if $e, e' \in M$ are neutral elements, then $e = e \cdot e' = e'$.)

1). (Generalised associative law) Let $a_1, \ldots, a_n \in M$ and let $p = a_1 \cdot a_2 \cdot \cdots \cdot a_n$ be recursively defined by $p_0 := e$, $p_{i+1} = p_i \cdot a_{i+1}$, $i = 0, 1, \ldots, n-1$ and $p := p_n$. Then the value of p does not change if we choose another arbitrary brackets instead of the left- brackets that are used in the definition of p . Therefore in the multiplicative (resp. additive) notation this product is simply denoted by $\prod_{i=1}^{n} a_i = a_1 \cdot \cdots \cdot a_n$ (resp. $\sum_{i=1}^{n} a_1 = a_1 + \cdots + a_n$. (**Hint :** Prove the independance of the bracket by induction.)

2). (Generalised commutative law) Suppose that the binary operation $\cdot$ on M is commutative. Then the product $a_1 \cdot \cdots \cdot a_n$ is independent of the order of the elements $a_1, \ldots, a_n$. In this case for arbitrary family a_i , $i \in I$, of element of M , the product is simply denoted by $\prod_{i=1}^{n} a_i$ (in the multiplicative notation) and by $\sum_{i=1}^{n} a_i$ (in the additive notation).

3). If a_{ij} , $i \in I$, $j \in J$, is family of elements in a monoid M and if I and J are finite indexed sets, then we have : $\displaystyle\sum_{(i,j)\in I\times J} a_{ij} = \sum_{i\in I}\Big(\sum_{j\in J} a_{ij}\Big) = \sum_{j\in J}\Big(\sum_{i\in I} a_{ij}\Big)$ In particular, $\displaystyle\sum_{\substack{1\leq i\leq m\\ 1\leq j\leq n}} a_{ij} = \sum_{i=1}^{m}\Big(\sum_{j=1}^{n} a_{ij}\Big) = \sum_{j=1}^{n}\Big(\sum_{i=1}^{m} a_{ij}\Big)$.

(**Hint :** The prrof is clear from the following scheme :

$$\begin{array}{r|l} a_{11} + a_{12} + \cdots + a_{1n} & \sum_{j=1}^{n} a_{1j} \\ + a_{21} + a_{22} + \cdots + a_{2n} & + \sum_{j=1}^{n} a_{2j} \\ \vdots & \vdots \\ + a_{m1} + a_{m2} + \cdots + x_{mn} & + \sum_{j=1}^{n} a_{mj} = \sum_{i=1}^{m}(\sum_{j=1}^{n} a_{ij}) \\ \hline \sum_{i=1}^{m} a_{i1} + \sum_{i=1}^{m} a_{i2} + \cdots + \sum_{i=1}^{m} a_{in} & \\ = \sum_{j=1}^{n}(\sum_{i=1}^{m} a_{ij}) & \end{array} \qquad)$$

4). An element $a' \in M$ is called a inverse of an element $a \in M$ if $a \cdot a' = a' \cdot a = e$. An element $a \in M$ is called invertible or unit if a has inverse in M . The set of invertible elements in m is denoted by $M^\times$.

a). If an element $a \in M$ is invertible, then there is only one inverse of a . (**Hint :** if $a', a'' \in M$ are two inverses of a , then $a' = e \cdot a' = (a'' \cdot a) \cdot a' = a'' \cdot (a \cdot a') = a'' \cdot e = a''$.) In the multiplicative notation the inverse of a invertible element $a \in M$ is denoted by a^{-1} . In the additive notation the inverse of a invertible element $a \in M$ is also called the negative and is denoted by $-a$.

b). In the monoids $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ every element is invertible and in the monoid $\mathbb{N}, +)$ the only element which is invertible is 0 , i.e. $(\mathbb{Z}, +)^\times = \mathbb{Z}$ $(\mathbb{Q}, +)^\times = \mathbb{Q}$ and $(\mathbb{N}, +)^\times = \{0\}$. For the multiplicative monoids $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$ and $(\mathbb{N}, \cdot)$, we have $(\mathbb{Z}, \cdot)^\times = \{1, -1\}$ $(\mathbb{Q}, \cdot)^\times = \mathbb{Q} \setminus \{0\}$ and $(\mathbb{N}, \cdot)^\times = \{1\}$.

c). Let X be a set and let X^X be the monoid of the set of all maps from X into itself with $\cdot = \circ$ the composition of maps. An element $\varphi \in X^X$ is invertible if and only if there exists $\varphi' \in X^X$ such that $\varphi \circ \varphi' = \varphi' \circ \varphi = \mathrm{id}_X$, or equivaletly, if and only if φ is bijective; in this case then $\varphi' = \varphi^{-1}$ is the inverse function of φ . In particular, $\left(X^X\right)^\times = \mathfrak{S}(X) =$ the set of all permutations of the set X .

d). (Rules for invertible elements) (i) $e \in M^\times$ and $e^{-1} = e$ (ii) If $a \in M^\times$, then $a^{-1} \in M^\times$ and $\left(a^{-1}\right)^{-1} = a$. (iii) If $a_1, \ldots, a_n \in M^\times$, then $a_1 \cdot \cdots \cdot a_n \in M^\times$ and $(a_1 \cdot \cdots \cdot a_n)^{-1} = a_n^{-1} \cdot \cdots \cdot a_1^{-1}$. In particular, if $a, b \in M^\times$, then $ab \in M^\times$ and $(ab)^{-1} = b^{-1}a^{-1}$.

e). The binary operation $\cdot$ of M induces a binary operation on $M^\times$, i.e. $M^\times$ is a submonoid of M. Moreover, in this submonoid every element is invertible. In particular, $(M^\times, \cdot)$ is a group; this group is called the group of invertible elements of $(M, \cdot)$. For example, for the monoid $(X^X, \circ)$, the group of invertible elements $\left((X^X)^\times, \circ\right)$ is the *permutation group* $\mathfrak{S}(X)$ on X.

5). (Powers of elements) For $a \in M$ and $n \in \mathbb{N}$, the n-power of a is the n-fold product of a with itself. If $a \in M^\times$, then we define $a^{-n} := (a^{-1})^n = (a^n)^{-1}$. In the additive notation this correspond to the multiples na of a. We have the following rules for the powers:

For all $a \in M$ and for all $m, n \in \mathbb{N}$ (in the case of group for all $m, n \in \mathbb{Z}$), we have:

(i) $a^{m+n} = a^m \cdot a^n$. (ii) $(a^m)^n = a^{mn}$. (iii) Moreover, if $a, b \in M$ are commute, then $a^m \cdot b^n = b^n \cdot a^m$ and $(a \cdot b)^m = a^m \cdot b^m$.

In the additive notation, we have: (i) $(m+n)a = ma + na$. (ii) $n(ma) = (mn)a = (nm)a$.

(iii) $ma + nb = nb + ma$ and $m(a+b) = ma + mb$. (In the additive notation one usually assume that M is commutative.

6). Let $(M, \cdot)$ be a monoid with neutral element e. Then:

a). For an element a in a monoid M, the following statements are equivalent:

(i) a is invertible. (ii) The left translation $\lambda_a : M \to M$, $x \mapsto a \cdot x$ is bijective. (iii) The right translation $\varrho_a : M \to M$, $x \mapsto x \cdot a$ is bijective.

b). If $a \in M$ has a left-inverse a' (i.e. $a' \cdot a = e$) and has a right-inverse a'' (i.e. $a \cdot a'' = e$), then a is invertible with $a^{-1} = a' = a''$. Deduce that: if a has more than one right-inverse (resp. left-inverse), then a has no left-inverse (resp. right-inverse).

c). Let $\varphi, \psi \in \mathbb{N}^\mathbb{N}$ be defined by $\varphi(0) := 0$, $\varphi(n) := n - 1$ if $n \geq 1$, and $\psi(n) := n + 1$ respectively. Then in the monoid $(\mathbb{N}^\mathbb{N}, \circ)$, the element φ is a left- inverse of ψ and the element ψ is a right-inverse of φ, i,e., $\varphi \circ \psi = \mathrm{id}_\mathbb{N}$ and the element ψ has infinitely many left-inverses in $\mathbb{N}^\mathbb{N}$ and in particular, ψ is not invertible. Further, in the submonoid of $\mathbb{N}^\mathbb{N}$, generated by ψ and φ (i.e., the smallest submonoid of $\mathbb{N}^\mathbb{N}$ containing ψ and φ) ψ is not invertible, even if ψ has exactly one left-inverse (namely φ).

7). (Cancellative Monoid) A monoid M is said to be regular or cancellative if for all $a, b, c \in M$, both the implications hold: (i) $ab = ac \Rightarrow b = c$. (ii) $ba = ca \Rightarrow b = c$.

An element $a \in M$ is called regular if the left- translation map $\lambda_a : M \to M$ and the right-transaltion map $\rho_A : M \to M$ are injective. Let $M^* := \{a \in M \mid a \text{ is regular in } M\}$ of regular elements in M is a submonoid of M. Therefore M is a cancellative monoid if and only if every element in M is regular, i.e., $M^* = M$.

8). Let M be a monoid and let $a_1, \ldots, a_n$ be elements in M be such that the product $a_1 \cdot \cdots \cdot a_n$ invertible. In the following cases all of $a_1, \ldots, a_n$ are invertible:

(i) The $a_1, \ldots, a_n$ are pairwise commute. (ii) M is finite. (iii) M is cancellative.

9). (Groups) A monoid $(M, \cdot)$ is called a group if $(M^\times, \cdot) = (M, \cdot)$, i.e. every element in M is invertible. Therefore a group is a set G together with an associative binary operation together $\cdot$ and an element e such that the following conditions are satisfied:

(i) e is a neutral element, i.e., $ea = ae = a$ for all $a \in G$. (ii) For every $a \in G$, there exists an inverse, i.e., an element $a' \in G$ such that $aa' = a'a = e$.

a). For a *semi-group* $(M, \cdot)$ (i.e. the binary operation $\cdot$ on the set M is associative) with an element e, the following statements are equivalent:

(i) e is a right-neutral element, i.e., $ae = a$ for all $a \in M$. (ii) For all $a \in M$, there exists a right-inverse, i.e., there exists an element $a' \in M$ such that $aa' = e$.

Then show that $(M, \cdot)$ is a group. (**Hint:** *e is a neutral element in M* : Let $a \in M$ be an arbitrary element and let $a', a'' \in M$ (these elements exist by the assumption (ii)) be such that $aa' = e$ and $a'a'' = 1$. Then $a = ae = a(a'a'') = (aa')a'' = ea''$ and hence $a = ea'' = (ee)a'' = e(ea'') = ea$. Further, since $aa' = e$, we need only to prove that $a'a = e$; this follows from $a = ea'' = a''$ which is proved above.) (**Remark:** Naturally, the above assertion is true if we replace "right-neutral" and "right- inverse" by "left-neutral" and "left-inverse" respectively.)

b). Let $(G, \cdot)$ be a semi-group with the following two properties:

(i) For every $a \in G$, the left-translation map $\lambda_a : G \to G$, $x \mapsto ax$, is surjective. (ii) There exist an element $b \in G$, the right-translation map $\rho_b : G \to G$, $x \mapsto xb$, is surjective.

Then show that $(G, \cdot)$ is a group.(**Hint:** Use exercise a) above.)

c). Construct a semi-group $(H, \cdot)$ with an element $e \in H$, which is *not* a group and satisfies the following properties: (i) $ea = a$ for all $a \in H$. (ii) for every $a \in H$ there exists an element $a' \in H$ with $aa' = e$.

d). If every equation of the form $a \cdot x = b$ with $a, b \in M$ has a solution in M, i.e. there exists and element $x \in M$ such that $a \cdot x = b$, then $(M, \cdot)$ is a group.

e). For $a, b \in \mathbb{R}$, let $f_{a,b} : \mathbb{R} \to \mathbb{R}$ be defined by $f_{a,b}(x) = ax + b$, $x \in \mathbb{R}$. Then $G := \{f_{a,b} \mid a, b \in \mathbb{R},\ a \neq 0\}$ with the binary operation $\circ$ of composition of maps. Show that $(G, \circ)$ is a group which is not commutative. (**Remark:** This is the well-known affine group of $\mathbb{R}$ usually denoted by $\mathrm{A}_1(\mathbb{R})$ and is used to study *affine geometry*.)

f). Let G be a finite group with n elements and let $(a_1, \ldots, a_n) \in G^n$. Show that there exist r, s with $1 \leq r, s \leq n$ such that $a_{r+1} \cdot \cdots \cdot a_s = e_G$. (**Hint:** The $n + 1$ products $a_1 \cdot \cdots \cdot a_s$, $s = 0, \ldots, n$ cannot be distinct.)

g). Let G be a finite abelian group with identity element e and with only one element f of order 2. Then $\operatorname{Ord} G = 2n$ with $n \in \mathbb{N}^*$. Further,

(i) $\prod_{x \in G} x = f$.

(ii) Let $a \in G$. If there exists an element $b \in G$ with $b^2 = a$, then $a^n = e$, in the other case $a^n = f$. (**Hint:** If a is not a square in G, then the relation: $c \sim d$ if and only if $c = d$ or $cd = a$ is an equivalence relation in G, all the equivalence classes contain exactly two elements. Let $K(1), \ldots, K(n)$ be these equivalence classes. Then $a^n = \prod_{i=1}^{n} (\prod_{y \in K(i)} y) = \prod_{x \in G} x = f$.)

10). Let N be a monoid, $a \in N$ and let $M = \{a^n \mid n \in \mathbb{N}\}$ be a submonoid of N generated by a. Suppose that the powers a^n, $n \in \mathbb{N}$ are not distinct. Let $m \in \mathbb{N}$ be the smallest natural number with $a^{m+1} \in \{a^0, a, \ldots, a^m\}$ and let r be an integer with $-1 \leq r < m$ and $a^{m+1} = a^{r+1}$. Then $H := \{a^n \mid n > r\} = \{a^{r+1}, \ldots, a^m\}$ is a cyclic subgroup of N of order $m - r$. (**Hint:** For $s, t > r$, we have $a^s = a^t \iff s \equiv t \bmod (m - r)$. It follows that every element a^s with $s \equiv 0 \bmod (m - r)$ is the neutral element and every element a^t with $t > r$ and $\gcd(t, m - r) = 1$ generates every element of H.) Other than $\{a^0\}$, the subgroups of H are the only semi-groups of M which are groups. (**Hint:** The equations $a^s = xa^t$, $t > s$ have solutions in M only if $s > r$.)

11). A finite monoid N with neutral element e is a group if and only if the only element $a \in N$ which satisfies $a^2 = a$ is the neutral element, i.e. $\{a \in N \mid a^2 = a\} = \{e\}$.

T3.2. (Rings) Let $A = (A, +, \cdot)$ be a ring. The group $(A, +)$ is called the additive group of A and the monoid $(A, \cdot)$ is called the monoid of A. The neutral element of A with repsect to the addition (resp. multiplication) is called the zero-element (resp. the unity or the unit-element) of A and is denoted by 0_A or just by 0 (resp. 1_A or just by 1).

1). (Rule for calculation) For all $a, b \in A$ and $m, n \in \mathbb{Z}$ we have:

(i) $a \cdot 0 = 0 \cdot a = 0$. (ii) $a(-b) = (-a)b = -ab$. (iii) $(-a)(-b) = ab$. (iv) $(m+n)a = ma + na$. (v) $m(a + b) = ma + mb$. (vi) $(mn)a = m(na)$. (vii) $(ma)(nb) = (mn)(ab)$.

(**Remarks:** By the rule (vii) above, the integral multiple ma of an element a in a ring A, can be identified with the product $(m1_A)a$ of the multiple $m1_A$ of the identity element 1_A of A with a. In particular, if $m1_A = 0$, then $ma = 0$ for all $a \in A$. If there is no misunderstanding, one writes just m for the element $m1_A$ of A.)

2). (Power-set ring) Let X be any set. Show that: if $X \neq \emptyset$, then the power set $(\mathfrak{P}(X), \cup, \cap)$ with union $\cup$ as addition and the intersection $\cap$ as multiplication not a ring. But $(\mathfrak{P}(X), \Delta, \cap)$ with the symmetric difference $A \Delta B := (A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A)$, $A, B \in \mathfrak{P}(X)$, as addition and the intersection $\cap$ as multiplication is a ring; this ring is called the power-set ring of X. Further, it is a commutative ring and the zero element is the empty set $\emptyset$ and the identity element is the set X. If X is finite, then $\mathfrak{P}(X)$ is a ring with $2^{|X|}$ elements. For $|X| = 1$ the operation tables of the addition and the multiplication in $\mathfrak{P}(X)$ are:

$+$	$\emptyset$	X
$\emptyset$	$\emptyset$	X
X	X	$\emptyset$

$\cdot$	$\emptyset$	X
$\emptyset$	$\emptyset$	$\emptyset$
X	$\emptyset$	X

.

3). (Opposite ring) Let A be a ring. If one defines the opposite multiplication in A by using the given multiplication on A by $(a, b) \mapsto ba$, then one obtains a ring, and this ring is called the ring with opposite multiplication or the opposite ring. It is denoted by A^{op} or by A^{o}. We have $(A^{\mathrm{op}})^{\mathrm{op}} = A$. If A is commutative, then $A = A^{\mathrm{op}}$.

4). (Direct product of rings) Let A_i, $i \in I$, be a family of rings with zero elements $0_i \in A_i$ and identity elements $1_i \in A_i$. The product of multiplications in A_i defines a multiplication in the product group $\prod_{i \in I} A_i$.

With this multiplication $\prod_{i\in I} A_i$ is a ring with the zero element $(0_i)_{i\in I}$ and the identity element $(1_i)_{i\in I}$. This ring is called the direct product of the rings A_i, $i \in I$. The direct sum $\bigoplus_{i\in I} A_i (\subseteq \prod_{i\in I} A_i)$ of the additive groups A_i is closed with respect to the above multiplication. But if the rings A_i, $i \in I$, are non-zero for infinitely many $i \in I$, then $\bigoplus_{i\in I} A_i$ with the operations induced from $\prod_{i\in I} A_i$ is not a ring: there is no identity element for the multiplication!

5). (Rings without unity) In our definition of ring, we assume the existence of a neutral element with respect to the multiplication. One can extend this definition by assuming only, that a ring with respect to the multiplication form only a semigroup. Then we can consider rings not necessarily with unity. From a ring A, which is not necessarily with unit element, one can easily construct a ring with unity. For example, on the set $\mathbb{Z} \times A$, define addition and multiplication by

$$(m, a) + (n, b) := (m + n,\ a + b) \text{ and } (m, a) \cdot (n, b) := (mn,\ mb + na + ab)$$

for $m, n \in \mathbb{Z}$ and $a, b \in A$. With these binary operations $\mathbb{Z} \times A$ is a ring with the unity $(1, 0)$. With this passage from A to $\mathbb{Z} \times A$ the assertions, which hold in a ring, frequently hold in rings, which does not have unity.

6). (General distributivity theorem) If a_i, $i \in I$, and b_j, $j \in J$, are two families of elements in a ring A and if $a_i = 0$ for almost all $i \in I$ and $b_j = 0$ for almost all $j \in J$, then $a_i b_j = 0$ for almost all $(i, j) \in I \times J$, and we have $\Big(\sum_{i\in I} a_i\Big)\Big(\sum_{j\in J} b_j\Big) = \sum_{(i,j)\in I\times J} a_i b_j$. In particular, $\Big(\sum_{i=1}^{m} a_i\Big)\Big(\sum_{j=1}^{n} b_j\Big) = \sum_{\substack{1\le i\le m\\ 1\le j\le n}} a_i b_j$

(**Hint:** Proof follows from the following scheme:

$$\begin{array}{r|l}
a_1b_1 + a_1b_2 + \cdots + a_1b_n & a_1 \sum_{j=1}^{n} b_j \\
+\ a_2b_1 + a_2b_2 + \cdots + a_2b_n & +a_2 \sum_{j=1}^{n} b_j \\
\vdots & \vdots \\
+\ a_mb_1 + a_mb_2 + \cdots + x_my_n & +a_m \sum_{j=1}^{n} b_j \\
\hline
 & = \big(\sum_{i=1}^{n} a_i\big)\big(\sum_{j=1}^{n} b_j\big). \qquad)
\end{array}$$

T3.3. **1).** Determine the last digit in the decimal expansion of 77^{77}.

2). Determine the last two digit in the decimal expansion of 9^{9^9}.

3). For every $n \in \mathbb{Z}$, show that $n^8 - n^2$ is divisble by 252. (**Hint:** $n^8 - n^2 = 0$ in all prime rings A_q for every prime divisor of 252.)

4). Let a and b be non-zero relatively prime integers. Then the sum $a^{\varphi(|b|)} + b^{\varphi(|a|)} \equiv 1 \mod ab$.

5). Determine all natural multiples of the number 17 for which the digits in the decimal expansion are all equal to 1. (**Hint:** Make calculation in the unit group $\mathrm{A}_{17}^{\times}$.)

---

† **Adolf Abraham Halevi Fraenkel (1891-1965)** was born on 17 Feb 1891 in Munich, Germany and died on 15 Oct 1965 in Jerusalem, Israel. Adolf Fraenkel, in common with most students in Germany in his time, studied for periods at different universities. He spent some time at the University of Munich, the University of Marburg, the University of Berlin and the University of Breslau. From 1916 he lectured at the University of Marburg, being promoted to professor there in 1922. In 1928 Fraenkel left Marburg and spent one year teaching at the University of Kiel. He was a fervent Zionist and, after leaving Kiel, he taught at the Hebrew University of Jerusalem from 1929. Fraenkel was to spend the rest of his career at the Hebrew University.

Fraenkel's first work was on "Hensel's p-adic numbers" and on the "theory of rings". However he is best known for his work on set theory, writing his first major work on the topic "Einleitung in die Mengenlehre" in 1919. He made two attempts, in 1922 and 1925, to put set theory into an axiomatic setting that avoided the paradoxes. He tried to improve the definitions of Zermelo and, within his axiom system, he proved the independence of the axiom of choice. His system of axioms was modified by Skolem in 1922 to give what is today known as the ZFS system. This is named after Zermelo, Fraenkel and Skolem. Within this system it is harder to prove the independence of the axiom of choice and this was not achieved until the work of Cohen in 1963.

Fraenkel was also interested in the history of mathematics and wrote a number of important works on the topic. He wrote on Gauss's work in algebra in 1920, then in 1930, he published an important biography of Cantor. In 1960 he published "Jewish mathematics and astronomy". A number of Fraenkel's students have made important contributions to mathematics including Robinson who succeeded him when he retired from his chair at the Hebrew University.