# Basic Algebra

## 1. Rings[1])

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)**

**1.1.** For $n \in \mathbb{N}^*$, let $Z_n$ denote a cyclic (additively written) group of order $n$. If $N \subseteq \mathbb{N}^*$ is an infinite subset of the set of positive natural numbers, then the additive group $\bigoplus_{n\in N} Z_n$ is not a ring (with unity) with any multiplication.

**1.2.** (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 $\varepsilon$, 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 $\varepsilon$ 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 $\zeta$ 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:

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

**d).** In the special case $A = \mathbb{Z}$, in addition to the numerical functions $\varepsilon$ and $\zeta$, the important Euler's $\varphi$-function $\varphi$, 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

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

[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).

(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.)

**1.3.** (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 $\operatorname{Inv}(A)$ denote the set of all (with respect to the multiplication of $A$) involutory elements, $\operatorname{Idp}(A)$ be the set of all idempotent elements of $A$. Then the map

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

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 $\gamma$ is a group homomorphism of the additive group $\operatorname{Idp}(A)$ (see T1.5 below), into the multiplicative group $\operatorname{Inv}(A)$.)

**1.4.** Let $A$ be a ring and let $\alpha$, $\alpha' : A \to A$ 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: 1. $a = s + t$. 2. $s$ is idempotent, $t$ is nilpotent. 3. $s$ 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 (2) and (3), then $\alpha(a)$ must be nilpotent.) (**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 $\alpha$ 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 (2) and (3), one can apply T1.4 and conclude that $s$ and $t$ are unique.)

Below one can see (simple) test-exercises.

## Test-Exercises

**T1.1.** Let $A$ be a ring with $\operatorname{Char} A \neq 1, \neq 2$. If the unit group $A^\times$ of $A$ is cyclic, then $A^\times$ is finite and $|A^\times|$ is an even number.

**T1.2.** Let $A$ be a ring. If $u \in A$ is unipotent, then so is $u^{-1}$. If $u, v \in A$ are unipotent and commute, then $uv$ is also unipotent. If $A$ is commutative, then the set of unipotent elements in $A$ is a subgroup of $A^\times$.

**T1.3.** 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 $\gcd(p, \operatorname{Ord} a) = 1$.

**T1.4.** Let $a$, $b$ be idempotent elements in a ring $A$.

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

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

**c).** If $ab = ba$ and $a - b$ nilpotent, then $a = b$.

**T1.5.** Let $A$ be a commutative ring and $\operatorname{Idp}(A)$ be the set of all idempotent elements in $A$. Then $(\operatorname{Idp}(A), \triangle, \cdot)$ is a Boolean ring, with the addition $a \triangle b := (a - b)^2$ and the multiplication induced from the multiplication from $A$. (the rings $(\operatorname{Idp}(A), \triangle, \cdot)$ and $(A, +, \cdot)$ are equal if and only if $A$ if $A$ is a Boolean ring).

† **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.