Course 2

Algebraic structures

Prof. dr. Septimiu Crivei

Chapter 1. Preliminaries

Application: fast adding

We describe a method for fast adding large natural numbers, following [Lidl, Pilz].

If $a, b \in \mathbb{N}$, then it makes no difference if we add them in $\mathbb{N}$ or in some group $(\mathbb{Z}_n, +)$ of residue classes modulo n with $n > a + b$.

By the forthcoming Chinese Remainder Theorem, it allows one (the computer) to replace the addition of large natural numbers by parallel "small" simultaneous additions. This technique is used in the design of computer software in order to speed up calculations.

$$\begin{aligned} a = 37 \to [37]_{140} \to ([37]_4, [37]_5, [37]_7) &= ([1]_4, [2]_5, [2]_7) \quad + \\ b = 56 \to [56]_{140} \to ([56]_4, [56]_5, [56]_7) &= ([0]_4, [1]_5, [0]_7) \\ a + b \qquad\qquad\qquad\qquad\qquad\qquad &= ([1]_4, [3]_5, [2]_7) \end{aligned}$$

Operations

Definition

By an *operation* (or *composition law*) on a set A we understand a function

$$\varphi : A \times A \to A.$$

Usually, we denote operations by symbols like $\cdot$, $+$, $*$, so that $\varphi(x, y)$ is denoted by $x \cdot y$, $x + y$, $x * y$, $\forall (x, y) \in A \times A$. We denote by $(A, \cdot)$ the fact that " $\cdot$ " is an operation on a set A.

Example

Are the usual addition and multiplication operations on $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$? What about the usual subtraction and division?

Operation laws

Definition

Let " $\cdot$ " be an operation on an arbitrary set A.
(1) *Associative law*: $(x \cdot y) \cdot z = x \cdot (y \cdot z), \quad \forall x, y, z \in A$.
(2) *Commutative law*: $x \cdot y = y \cdot x, \quad \forall x, y \in A$.
(3) *Identity law*: $\exists e \in A$ such that $\forall a \in A,\ a \cdot e = e \cdot a = a$. In this case, e is called an *identity element*.
(4) *Inverse law*: $\forall a \in A, \exists a' \in A$ such that $a \cdot a' = a' \cdot a = e$, where e is the identity element. In this case, a' is called an *inverse element for a*.

Lemma

Let " $\cdot$ " be an operation on a set A.
(i) If there exists an identity element in A, then it is unique.
(ii) Assume further that the operation " $\cdot$ " is associative and has identity element e and let $a \in A$. If an inverse element for a does exist, then it is unique.

Stable (closed) subsets

Definition

Consider an operation $\varphi : A \times A \to A$ on a set A and let $B \subseteq A$. Then B is called a *stable subset of A with respect to φ* (or *closed subset of A under the operation φ*) if

$$\forall x, y \in B\,, \quad \varphi(x, y) \in B\,.$$

In this case, we may consider the operation $\varphi' : B \times B \to B$ on B defined by

$$\varphi'(x, y) = \varphi(x, y)\,, \quad \forall (x, y) \in B \times B\,,$$

called the *operation induced by φ in the stable subset B of A*. When using a symbol "$\cdot$" for φ, we simply say that B *is a stable subset of* $(A, \cdot)$.

Examples

Example

(*a*) Are the sets $2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$ and $2\mathbb{Z}+1 = \{2k+1 \mid k \in \mathbb{Z}\}$ stable in $(\mathbb{Z}, +)$?

(*b*) Are the intervals $[0, 1]$ and $[-1, 0]$ stable in $(\mathbb{R}, \cdot)$?

The associative, the commutative (and later on, the distributive laws) still hold in a stable subset (endowed with the induced operation), since they are true for every element in the initial set (only the universal quantifier $\forall$ appears in their definition). But the identity element and the inverse element do not transfer (their definition uses the existential quantifier $\exists$ as well).

Definition

Let " $\cdot$ " be an operation on a set A. Then $(A, \cdot)$ is called a:
(1) *semigroup* if the associative law holds.
(2) *monoid* if it is a semigroup with identity element.
(3) *group* if it is a monoid in which every element has an inverse.

If the operation is commutative as well, then the structure is called *commutative*. A commutative group is also called an *abelian group* (after the name of N. H. Abel).

Remark

We denote by 1 the identity element of a group $(G, \cdot)$ and by x^{-1} the inverse of an element $x \in G$. In case of an additive group $(G, +)$, the identity element is denoted by 0, while the inverse of an element $x \in G$ is called the *symmetric* of x and is denoted by $-x$.

Definition

Let $(G, \cdot)$ be a semigroup, let $x \in G$ and let $n \in \mathbb{N}^*$. Then we may use the associative law and define

$$x^n = \underbrace{x \cdot x \cdot \ldots \cdot x}_{n \text{ times}}.$$

If $(G, \cdot)$ is a monoid, then we may also define $x^0 = 1$.
If $(G, \cdot)$ is a group, then we may also define $x^{-n} = (x^{-1})^n$.

If the operation is "+", then x^n becomes nx.

Properties in groups

Lemma

Let $(G, \cdot)$ be a group, let $x \in G$ and let $m, n \in \mathbb{Z}$. Then:
(i) $x^m \cdot x^n = x^{m+n}$.
(ii) $(x^m)^n = x^{mn}$.

Lemma

Let $(G, \cdot)$ be a group and let $a, x, y \in G$. Then:
(i) $a \cdot x = a \cdot y \Longrightarrow x = y$,
$x \cdot a = y \cdot a \Longrightarrow x = y$ *(cancellation laws).*
(ii) $(x^{-1})^{-1} = x$.
(iii) $(x \cdot y)^{-1} = y^{-1} \cdot x^{-1}$.

A finite group may be defined by its operation table, that specifies the result of any multiplication of two elements. By cancellation laws, the operation table of a group has the property that every element appears exactly once on each row and each column.

Examples I

(a) The operation "$-$" defined on $\mathbb{Z}$ is not associative.

(b) $(\mathbb{N}^*, +)$ is a semigroup, but not a monoid.

(c) $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$ are monoids, but not groups.

(d) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$ and $(\mathbb{C}^*, \cdot)$ are groups.

(e) Let X be a non-empty set. By a *word on* X of length n we understand a string of n elements from X for some $n \in \mathbb{N}$. The word of length 0 is called the *void word* and is denoted by e. On the set X^* of words on X consider the operation "$\cdot$" given by concatenation. Then $(X^*, \cdot)$ is a monoid with identity element e, called the *free monoid* on the set X.

Examples II

(f) Let $\{e\}$ be a single element set and let "$\cdot$" be the only operation on $\{e\}$, defined by $e \cdot e = e$. Then $(\{e\}, \cdot)$ is an abelian group, called the *trivial group*.

(g) Let $n \in \mathbb{N}$, $n \geq 2$. Then $(\mathbb{Z}_n, +)$ is an abelian group, called the *group of residue classes modulo n*. The addition is defined by

$$\widehat{x} + \widehat{y} = \widehat{x + y}\,, \quad \forall \widehat{x}, \widehat{y} \in \mathbb{Z}_n\,.$$

(h) Let $n \in \mathbb{N}$ with $n \geq 2$. Denote by $M_{m,n}(\mathbb{R})$ the set of $m \times n$-matrices with entries in $\mathbb{R}$ and by $M_n(\mathbb{R})$ the set of $n \times n$-matrices with entries in $\mathbb{R}$. Then $(M_{m,n}(\mathbb{R}), +)$ is an abelian group and $(M_n(\mathbb{R}), \cdot)$ is a monoid.
Denote by $GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det(A) \neq 0\}$ the set of invertible $n \times n$-matrices with real entries. Then $(GL_n(\mathbb{R}), \cdot)$ is a group, called the *general linear group of rank n*.

Examples III

(i) Let M be a set and let $S_M = \{f : M \to M \mid f \text{ is bijective}\}$. Then $(S_M, \circ)$ is a group, called the *symmetric group of* M. The identity element is the identity map 1_M and the inverse of an element f (which is a bijection) is the inverse function f^{-1}.
If $|M| = n$, then S_M is denoted by S_n, and the group $(S_n, \circ)$ is in fact the *permutation group* of n elements.

(j) Let $K = \{e, a, b, c\}$ and define an operation " $\cdot$ " on K by the following table:

$\cdot$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

Examples IV

Then $(K, \cdot)$ is an abelian group, called *Klein's group*. It may be viewed as the group of geometric transformations of a rectangle:

- e is the identical transformation,
- a is the symmetry with respect to the horizontal symmetry axis,
- b is the symmetry with respect to the vertical symmetry axis,
- c is the symmetry with respect to the center of the circumscribed circle.

The product $x \cdot y$ is defined by performing first y and then x.

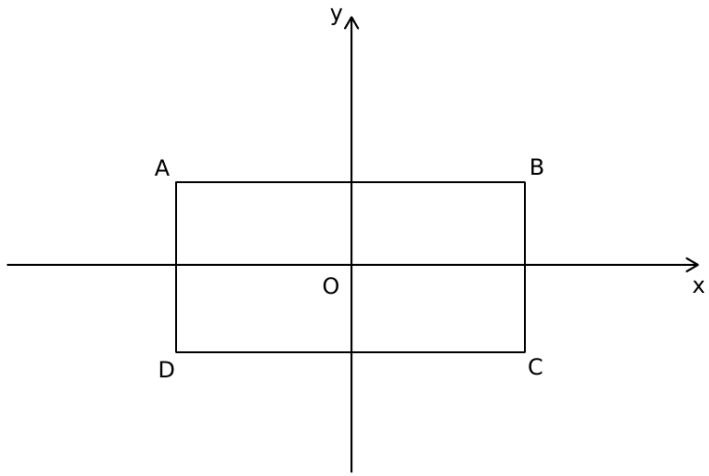

Figure: Klein's group.

Definition

Let R be a set. A structure with two operations $(R, +, \cdot)$ is called a:
(1) *ring* if $(R, +)$ is an abelian group, $(R, \cdot)$ is a semigroup and the *distributive laws* hold:

$$x \cdot (y + z) = x \cdot y + x \cdot z, \quad \forall x, y, z \in R,$$
$$(y + z) \cdot x = y \cdot x + z \cdot x, \quad \forall x, y, z \in R.$$

(2) *unitary ring* if $(R, +, \cdot)$ is a ring and there is an identity element with respect to " $\cdot$ ".
(3) *division ring* (or *skew field*) if $(R, +)$ is an abelian group, $(R^*, \cdot)$ is a group and the distributive laws hold.
(4) *field* if it is a commutative division ring.
The ring $(R, +, \cdot)$ is called *commutative* if " $\cdot$ " is commutative.

If $(R, +, \cdot)$ is a ring, then we denote the identity elements with respect to "$+$" and "$\cdot$" by 0 and 1 respectively. We also use the notation $R^* = R \setminus \{0\}$.

A ring $(R, +, \cdot)$ is a division ring if and only if $|R| \geq 2$ and any $x \in R^*$ has an inverse $x^{-1} \in R^*$.

If $(R, +, \cdot)$ is a ring, then $(R, +)$ is a group and $(R, \cdot)$ is a semigroup, so that we may talk about multiples and positive powers of elements of R.

Definition

Let $(R, +, \cdot)$ be a ring, let $x \in R$ and let $n \in \mathbb{N}^*$. Then we define

$$n \cdot x = \underbrace{x + x + \cdots + x}_{n \text{ times}},$$

$$0 \cdot x = 0,$$

$$(-n) \cdot x = -n \cdot x,$$

$$x^n = \underbrace{x \cdot x \cdot \ldots \cdot x}_{n \text{ times}}.$$

If R is a unitary ring, then we may also consider $x^0 = 1$.
If R is a division ring, then we may also define $x^{-n} = (x^{-1})^n$.

In the definition $0 \cdot x = 0$, the first 0 is the integer zero and the second 0 is the zero element of the ring R, that is, the identity element of the group $(R, +)$.

Properties in rings

The first computational properties of a ring $(R, +, \cdot)$ are the properties of the group $(R, +)$ and of the semigroup $(R, \cdot)$. Some relationship properties between the two operations are given in the following result, in which all zeros are the zero element of R.

Lemma

Let $(R, +, \cdot)$ be a ring and let $x, y, z \in R$. Then:

(i) $x \cdot (y - z) = x \cdot y - x \cdot z.$

$(y - z) \cdot x = y \cdot x - z \cdot x.$

(ii) $x \cdot 0 = 0 \cdot x = 0.$

(iii) $x \cdot (-y) = (-x) \cdot y = -x \cdot y.$

Examples I

(a) $(\mathbb{Z}, +, \cdot)$ is a unitary ring, but not a field.

(b) $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ and $(\mathbb{C}, +, \cdot)$ are fields.

(c) Let $\{e\}$ be a single element set and let both "$+$" and "$\cdot$" be the only operation on $\{e\}$, defined by $e + e = e$ and $e \cdot e = e$. Then $(\{e\}, +, \cdot)$ is a commutative unitary ring, called the *trivial ring*.

(d) Let $n \in \mathbb{N}$, $n \geq 2$. Then $(\mathbb{Z}_n, +, \cdot)$ is a commutative unitary ring, called the *ring of residue classes modulo n*. The addition and the multiplication are defined by

$$\widehat{x} + \widehat{y} = \widehat{x + y}\,, \quad \widehat{x} \cdot \widehat{y} = \widehat{x \cdot y}\,, \quad \forall \widehat{x}, \widehat{y} \in \mathbb{Z}_n.$$

Note that $(\mathbb{Z}_n, +, \cdot)$ is a field if and only if n is prime.

(e) Let $(R, +, \cdot)$ be a commutative unitary ring. Then $(R[X], +, \cdot)$ is a commutative unitary ring, called the *polynomial ring over R in*

the indeterminate X, where the operations are the usual addition and multiplication of polynomials.

(f) Let $n \in \mathbb{N}$, $n \geq 2$ and let $(R, +, \cdot)$ be a ring. Then $(M_n(R), +, \cdot)$ is a ring, called the *ring of matrices* $n \times n$ *with entries in* R, where the operations are the usual addition and multiplication of matrices.

(g) Let M be a non-empty set and let $(R, +, \cdot)$ be a ring. Define on the set

$$R^M = \{f \mid f : M \to R\}$$

two operations by: $\forall f, g \in R^M$, we have $f + g : M \to R$, $f \cdot g : M \to R$, where

$$(f + g)(x) = f(x) + g(x), \quad \forall x \in M,$$

$$(f \cdot g)(x) = f(x) \cdot g(x), \quad \forall x \in M.$$

Examples III

Then $(R^M, +, \cdot)$ is a ring, called the *ring of functions with a set as domain and a ring as codomain*. The zero element is $\theta : M \to R, \quad \theta(x) = 0, \quad \forall x \in M$. The symmetric of any $f : M \to R$ is $-f : M \to R, \quad (-f)(x) = -f(x), \quad \forall x \in M$.

(h) A ring $(R, +, \cdot)$ is called *Boolean* (after the name of G. Boole) if $a^2 = a$ for every $a \in R$. If M is a set and $\mathcal{P}(M)$ is the power set of M (that is, the set of all subsets of M), then $(\mathcal{P}(M), \Delta, \cap)$ is a Boolean ring, where Δ is the *symmetric difference* operation defined by

$$A \Delta B = (A \setminus B) \cup (B \setminus A)$$

for every $A, B \in \mathcal{P}(M)$.

Definition

Let $(G, \cdot)$ be a group and let $H \subseteq G$. Then H is called a *subgroup* of G if:
(i) H is a stable subset of $(G, \cdot)$.
(ii) $(H, \cdot)$ is a group.

We denote by $H \leq G$ the fact that H is a subgroup of a group G.

The next characterization theorem gives more efficient ways to check that a subset of a group is a subgroup.

Theorem

Let $(G, \cdot)$ be a group and let $H \subseteq G$. Then

$$H \leq G \Leftrightarrow \begin{cases} H \neq \emptyset \ (1 \in H) \\ \forall x, y \in H, \ x \cdot y \in H \\ \forall x \in H, \ x^{-1} \in H. \end{cases} \Leftrightarrow \begin{cases} H \neq \emptyset \ (1 \in H) \\ \forall x, y \in H, \ x \cdot y^{-1} \in H. \end{cases}$$

In case of an additive group $(G, +)$, the conditions become:

- $\forall x, y \in H, \ x + y \in H$.
- $\forall x \in H, \ -x \in H$.
- $\forall x, y \in H, \ x - y \in H$.

Examples I

(a) Every non-trivial group $(G, \cdot)$ has two subgroups, namely $\{1\}$ and G, called the *trivial subgroups*.

(b) $\mathbb{Z}$ is a subgroup of $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ and $(\mathbb{C}, +)$, $\mathbb{Q}$ is a subgroup of $(\mathbb{R}, +)$ and $(\mathbb{C}, +)$, $\mathbb{R}$ is a subgroup of $(\mathbb{C}, +)$.

(c) The set

$$n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$$

is a subgroup of $(\mathbb{Z}, +)$ for every $n \in \mathbb{N}$.

(d) The set

$$H = \{z \in \mathbb{C} \mid |z| = 1\}$$

is a subgroup of the group $(\mathbb{C}^*, \cdot)$, called the *circle group*. But it is not a subgroup of the group $(\mathbb{C}, +)$.

(e) The set

$$U_n = \{z \in \mathbb{C} \mid z^n = 1\} \quad (n \in \mathbb{N}^*)$$

is a subgroup of the group $(\mathbb{C}^*, \cdot)$, called the *group of n^{th} roots of unity*. Its elements are the following:

$$\varepsilon_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}, \quad k \in \{0, \ldots, n-1\}.$$

(f) Consider the general linear group $(GL_n(\mathbb{R}), \cdot)$ of rank n, where $GL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det(A) \neq 0\}$ $(n \in \mathbb{N},\ n \geq 2)$ and denote

$$SL_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid \det(A) = 1\}.$$

Then $SL_n(\mathbb{R})$ is a subgroup of $(GL_n(\mathbb{R}), \cdot)$, called the *special linear group of rank n*.

Subrings

Definition

Let $(R, +, \cdot)$ be a ring and let $A \subseteq R$. Then A is called a *subring* of R if:
(i) A is a stable subset of $(R, +, \cdot)$.
(ii) $(A, +, \cdot)$ is a ring.

Definition

Let $(K, +, \cdot)$ be a field and let $A \subseteq K$. Then A is called a *subfield* of K if:
(i) A is a stable subset of $(K, +, \cdot)$.
(ii) $(A, +, \cdot)$ is a field.

We denote by $A \leq R$ ($A \leq K$) the fact that A is a subring (subfield) of a ring R (field K).
In practice, one checks that a subset of a ring (field) is a subring (subfield) by using one of the next two characterization theorems.

Characterization of subrings

Theorem

Let $(R, +, \cdot)$ be a ring and let $A \subseteq R$. Then

$$A \text{ is a subring of } R \iff \begin{cases} A \neq \emptyset \ (0 \in A) \\ \forall x, y \in A, \ x - y \in A \\ \forall x, y \in A, \ x \cdot y \in A. \end{cases}$$

Theorem

Let $(K, +, \cdot)$ be a field and let $A \subseteq K$. Then

$$A \text{ is a subfield of } K \iff \begin{cases} |A| \geq 2 \ (0, 1 \in A) \\ \forall x, y \in A, \ x - y \in A \\ \forall x, y \in A \text{ with } y \neq 0, \ x \cdot y^{-1} \in A. \end{cases}$$

Examples

(a) Every non-trivial ring $(R, +, \cdot)$ has two subrings, namely $\{0\}$ and R, called the *trivial subrings*.

(b) $\mathbb{Z}$ is a subring of $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ and $(\mathbb{C}, +, \cdot)$.

(c) $\mathbb{Q}$ is a subfield of $(\mathbb{R}, +, \cdot)$ and $(\mathbb{C}, +, \cdot)$, while $\mathbb{R}$ is a subfield of $(\mathbb{C}, +, \cdot)$.

(d) The set

$$n\mathbb{Z} = \{nx \mid x \in \mathbb{Z}\}$$

is a subring of $(\mathbb{Z}, +, \cdot)$ for every $n \in \mathbb{N}$. Note that $n\mathbb{Z}$ does not have identity for $n \geq 2$.

(e) The set

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$$

is a subring of the field $(\mathbb{C}, +, \cdot)$, but not a subfield. It is called the *ring of Gauss integers*.

Group homomorphisms

We denote by the same symbol operations in different structures.

Definition

Let $(G, \cdot)$, $(G', \cdot)$ be groups and $f : G \to G'$. Then f is called a:

1. *group homomorphism* if $f(x \cdot y) = f(x) \cdot f(y)$, $\forall x, y \in G$.
2. *group isomorphism* if it is a bijective group homomorphism.

We denote by $G \simeq G'$ the fact that two groups G and G' are isomorphic. We denote by 1 and $1'$ the identity elements in G and G' respectively.

Theorem

Let $f : G \to G'$ be a group homomorphism. Then:
(i) $f(1) = 1'$.
(ii) $(f(x))^{-1} = f(x^{-1})$, $\forall x \in G$.

Examples

(a) Let $(G, \cdot)$ and $(G', \cdot)$ be groups and let $f : G \to G'$, $f(x) = 1'$, $\forall x \in G$. Then f is a group homomorphism, called the *trivial group homomorphism*.

(b) Let $(G, \cdot)$ be a group. Then $1_G : G \to G$ is a group isomorphism.

(c) Let $n \in \mathbb{N}$ and let $f : \mathbb{Z} \to \mathbb{Z}$ be defined by $f(x) = nx$. Then f is a group homomorphism from the group $(\mathbb{Z}, +)$ to itself.

(d) Let $n \in \mathbb{N}$ with $n \geq 2$. The map $f : \mathbb{Z} \to \mathbb{Z}_n$ defined by $f(x) = \widehat{x}$ is a group homomorphism between $(\mathbb{Z}, +)$ and $(\mathbb{Z}_n, +)$.

(e) Let $f : \mathbb{C}^* \to \mathbb{R}^*$, $f(z) = |z|$. Then f is a group homomorphism between $(\mathbb{C}^*, \cdot)$ and $(\mathbb{R}^*, \cdot)$. But $f : \mathbb{C} \to \mathbb{R}$, $f(z) = |z|$ is not a group homomorphism between $(\mathbb{C}, +)$ and $(\mathbb{R}, +)$.

(f) Let $n \in \mathbb{N}$, $n \geq 2$ and let $f : GL_n(\mathbb{R}) \to \mathbb{R}^*$, $f(A) = \det(A)$. Then f is a group homomorphism between $(GL_n(\mathbb{R}), \cdot)$ and $(\mathbb{R}^*, \cdot)$.

Definition

Let $(R, +, \cdot)$ and $(R', +, \cdot)$ be rings and $f : R \to R'$. Then f is called a:

1. *ring homomorphism* if $\forall x, y \in R$ we have

$$f(x + y) = f(x) + f(y),$$
$$f(x \cdot y) = f(x) \cdot f(y).$$

2. *ring isomorphism* if it is a bijective ring homomorphism.

We denote by $R \simeq R'$ the fact that two rings R and R' are isomorphic.

Examples

(*a*) Let $(R, +, \cdot)$ and $(R', +, \cdot)$ be rings and let $f : R \to R'$, $f(x) = 0'$, $\forall x \in R$. Then f is a ring homomorphism, called the *trivial ring homomorphism*.

(*b*) Let $(R, +, \cdot)$ be a ring. Then $1_R : R \to R$ is a ring isomorphism.

(*c*) Let $n \in \mathbb{N}$ with $n \geq 2$. The map $f : \mathbb{Z} \to \mathbb{Z}_n$, $f(x) = \widehat{x}$ is a ring homomorphism between $(\mathbb{Z}, +, \cdot)$ and $(\mathbb{Z}_n, +, \cdot)$.

(*d*) The map $f : \mathbb{C} \to \mathbb{R}$, $f(z) = |z|$ is not a ring (field) homomorphism between $(\mathbb{C}, +, \cdot)$ and $(\mathbb{R}, +, \cdot)$.

(*e*) Let $n \in \mathbb{N}$, $n \geq 2$ and let $f : M_n(\mathbb{R}) \to \mathbb{R}$, $f(A) = \det(A)$. Then f is not a ring homomorphism between $(M_n(\mathbb{R}), +, \cdot)$ and $(\mathbb{R}, +, \cdot)$.

Properties of ring homomorphisms

If $f : R \to R'$ is a ring homomorphism, then the first condition from its definition tells us that f is a group homomorphism between $(R, +)$ and $(R', +)$.

Then f takes the identity element of $(R, +)$ to the identity element of $(R', +)$, that is, $f(0) = 0'$ and we also have $f(-x) = -f(x)$, $\forall x \in R$.

But in general, even if R and R' have identities, denoted by 1 and $1'$ respectively, in general it does not follow that a ring homomorphism $f : R \to R'$ has the property that $f(1) = 1'$.

Unitary ring homomorphisms

Definition

Let $(R, +, \cdot)$ and $(R', +, \cdot)$ be rings with identity elements 1 and $1'$ respectively, and let $f : R \to R'$ be a ring homomorphism. Then f is called *unitary* if $f(1) = 1'$.

Theorem

Let $(R, +, \cdot)$ and $(R', +, \cdot)$ be unitary rings with identity elements 1 and $1'$ respectively, and let $f : R \to R'$ be a ring homomorphism.
(i) If f is surjective, then f is unitary.
(ii) If f is a ring isomorphism, then f is unitary.
(iii) If f is unitary and $x \in R$ has an inverse element $x^{-1} \in R$, then $f(x)$ has an inverse and

$$(f(x))^{-1} = f(x^{-1}).$$

Theorem (Chinese Remainder Theorem)

If $n = p_1^{r_1} \cdots p_k^{r_k}$ for some distinct primes $p_1, \ldots, p_k$, then there is an isomorphism of additive groups:

$$\mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}}$$

given by
$\varphi : \mathbb{Z}_n \to \mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}}, \quad \varphi([x]_n) = ([x]_{p_1^{r_1}}, \ldots, [x]_{p_k^{r_k}})$, *where* $[x]_m$ *denotes the residue class of* x *modulo* $m \in \mathbb{N}$. *If we denote* $n_i = p_i^{r_i}$, $N_i = \frac{n}{n_i}$ *and* $K_i = [N_i^{-1}]_{n_i}$ *for every* $i \in \{1, \ldots, k\}$, *then the inverse of* φ *is given by*

$$\psi : \mathbb{Z}_{p_1^{r_1}} \times \cdots \times \mathbb{Z}_{p_k^{r_k}} \to \mathbb{Z}_n, \quad \psi(a_1, \ldots, a_k) = \left[\sum_{i=1}^{k} a_i N_i K_i \right]_n .$$

Extra: Fast adding II

Let $a = 37$, $b = 56$, and choose $n = 140 = 2^2 \cdot 5 \cdot 7$.

$$\begin{aligned} a = 37 \to [37]_{140} \to ([37]_4, [37]_5, [37]_7) &= ([1]_4, [2]_5, [2]_7) \quad + \\ b = 56 \to [56]_{140} \to ([56]_4, [56]_5, [56]_7) &= ([0]_4, [1]_5, [0]_7) \\ a + b &= ([1]_4, [3]_5, [2]_7) \end{aligned}$$

Now one solves the following system by the *Chinese Remainder Theorem*:

$$\begin{cases} x = 1 \pmod 4 \\ x = 3 \pmod 5 \\ x = 2 \pmod 7 \end{cases}.$$

We have:

$$n_1 = 4, n_2 = 5, n_3 = 7, n = n_1 \cdot n_2 \cdot n_3 = 140,$$
$$N_1 = \frac{n}{n_1} = 35, N_2 = \frac{n}{n_2} = 28, N_3 = \frac{n}{n_3} = 20.$$

Note that $K_i = [N_i^{-1}]_{n_i}$ means that $N_i K_i = 1 \pmod{n_i}$.
Hence we have:

$$K_1 = N_1^{-1} \bmod n_1 = 35^{-1} \bmod 4 = 3^{-1} \bmod 4 = 3,$$
$$K_2 = N_2^{-1} \bmod n_2 = 28^{-1} \bmod 5 = 3^{-1} \bmod 5 = 7,$$
$$K_3 = N_3^{-1} \bmod n_3 = 20^{-1} \bmod 7 = 6^{-1} \bmod 7 = 6.$$

Finally, we get the solution

$$x = a_1 N_1 K_1 + a_2 N_2 K_2 + a_3 N_3 K_3 = 93$$

(unique solution modulo n). Hence $a + b = 93$.