

§18 Rings and fields

We want to combine "addition" and "multiplication"

- system of numbers $\mathbb{Z}, \mathbb{Q}, \dots$
- system of square matrixes M_n
- polynomials $p(X) = a_0 + a_1 X + \dots + a_n X^n$
- more general functions...

$\leadsto$ what should we expect for the interaction of two operations?

$$(a+b) \cdot c = a \cdot c + b \cdot c$$

Def. a ring is given by the following:

- set R
- binary operation $R \times R \rightarrow R$; write $a+b$
- another bin. op. $R \times R \rightarrow R$; write $a \cdot b$

such that:

- $(R, +)$ becomes a commutative group; write 0 for the identity elem. of this group structure
- $-a$ for the inverse of a , $a-b$ for $a+(-b)$
- so $a+0 = a = 0+a$, $0 = a+(-a) = a-a$
- the bin. op. $a \cdot b$ is associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c)$
- distributive law: $(a+b) \cdot c = a \cdot c + b \cdot c$
 $a \cdot (b+c) = a \cdot b + a \cdot c$

We often ~~write~~ write ab instead of $a \cdot b$

Ex. ring structure on $\mathbb{Z}_m$

$$[a] + [b] = [a+b] \quad (\text{the group structure})$$

$$[a] \cdot [b] = [ab]$$

$$\text{well-def'd by } [a] = [a'] \Rightarrow [ab] = [a'b] \text{ etc.} \\ \uparrow a - a' = mk$$

Non-ex. $\mathbb{N}$

Thm 18.8 R : ring a, b : elements of R

$$1. \quad 0 \cdot a = a \cdot 0 = 0$$

$$2. \quad a \cdot (-b) = (-a) \cdot b = -(ab)$$

$$3. \quad (-a) \cdot (-b) = ab$$

Proof for 1. set $c = 0 \cdot a$

$$\text{Step 1. } c + c = c$$

$$\text{use compute } (0+0) \cdot a$$

$$\text{Step 2. } c = 0$$

$$c = c + c + (-c) = c + (-c) = 0$$

Proof for 2. To check $a \cdot (-b) = -(ab)$

$$\text{it's enough to check } a \cdot (-b) + a \cdot b = 0$$

$$\text{left side: } a \cdot ((-b) + b) = a \cdot 0 = 0$$

Proof for 3. Use 2. twice to get $(-a) \cdot (-b) = -(-a \cdot b)$

Comparison of rings

a homomorphism of rings is a map $R \xrightarrow{\phi} R'$ s.t.

- $\phi(a+b) = \phi(a) +' \phi(b)$ hom. for the additive groups
- $\phi(a \cdot b) = \phi(a) \cdot' \phi(b)$ compat. with mult. bin. op.

Example $\mathbb{Z} \xrightarrow{\phi} \mathbb{Z}_m$ given by $\phi(n) = [n]$

We say two rings R, R' are isomorphic if there is a one-to-one & onto hom. $R \xrightarrow{\phi} R'$; write $R \cong R'$

Example m and n have no common divisors

$\leadsto \mathbb{Z}_{mn}$ and $\mathbb{Z}_m \times \mathbb{Z}_n$ are isom.

We already know that they are isom. as additive groups

$$(\text{Feb 11 } \S 11) \quad \text{by } \mathbb{Z}_{mn} \xrightarrow{\phi} \mathbb{Z}_m \times \mathbb{Z}_n \quad \phi([k]) = ([k], [k])$$

This is compatible with multiplication on both sides

Ring from group (from §24)

→ Consider the collection of "formal linear combinations"

$$a_1 g_1 + \dots + a_k g_k \quad a_i : \text{integer}, \quad g_i \in G$$

fix a group G commutativity of $+$

We have $a g + b g = (a+b)g$, $0 \cdot g = 0$ "empty sum"

but no other relations

→ We have a "multiplication" binary operation

$$(a_1 g_1 + \dots + a_k g_k) \cdot (b_1 h_1 + \dots + b_\ell h_\ell)$$

$$= \sum_{i=1}^k \sum_{j=1}^{\ell} a_i b_j \underbrace{(g_i h_j)}_{\text{computed in } G}$$

This is called the group ring $\mathbb{Z}G$ (also $\mathbb{Z}[G]$)

Rem. coefficients a_i can be from other number systems like "rational", "real", ...

then we write $\mathbb{Q}G$, $\mathbb{R}G$, ...

Idea behind the Fourier series

- Laurent polynomials $a_{-M} z^{-M} + \dots + a_N z^N$ $a_i \in \mathbb{C}$
(functions on $\{z \in \mathbb{C} \mid |z|=1\}$)

- elements of the group ring $\mathbb{C}\mathbb{Z}$
(just for now write $\mathbb{Z} = \{g^n \mid n \in \mathbb{Z}\}$
so $n \leftrightarrow g^n$)

$$a_{-M} g^{-M} + \dots + a_N g^N$$

can be identified $\mathbb{C}[z, z^{-1}] \simeq \mathbb{C}\mathbb{Z}$

1. The first part of the paper is devoted to the study of the

properties of the function $f(x)$ defined by the equation

$$f(x) = \int_0^x \frac{1}{1+t^2} dt$$

for $x \in \mathbb{R}$. It is shown that $f(x)$ is an odd function and

that $f(x)$ is bounded on $\mathbb{R}$. In the second part of the paper

we study the function $g(x)$ defined by the equation

$$g(x) = \int_0^x \frac{1}{1+t^4} dt$$

for $x \in \mathbb{R}$. It is shown that $g(x)$ is an even function and

that $g(x)$ is bounded on $\mathbb{R}$. In the third part of the paper

we study the function $h(x)$ defined by the equation

$$h(x) = \int_0^x \frac{1}{1+t^6} dt$$

for $x \in \mathbb{R}$. It is shown that $h(x)$ is an even function and

that $h(x)$ is bounded on $\mathbb{R}$. In the fourth part of the paper

we study the function $k(x)$ defined by the equation

$$k(x) = \int_0^x \frac{1}{1+t^8} dt$$

for $x \in \mathbb{R}$. It is shown that $k(x)$ is an even function and

that $k(x)$ is bounded on $\mathbb{R}$. In the fifth part of the paper

we study the function $l(x)$ defined by the equation

$$l(x) = \int_0^x \frac{1}{1+t^{10}} dt$$

for $x \in \mathbb{R}$. It is shown that $l(x)$ is an even function and

that $l(x)$ is bounded on $\mathbb{R}$. In the sixth part of the paper

we study the function $m(x)$ defined by the equation