Rings and fields.

Renzo's math 366

1 Definitions

1.1 Operations

A **(binary) operation** on a set X is a function from $\star : X \times X \to X$. It is common to denote the element $\star((x, y))$ as $x \star y$.

An operation $\star$ is:

associative if for every $x, y, z \in X$

$$x \star (y \star z) = (x \star y) \star z.$$

commutative if for every $x, y \in X$

$$x \star y = y \star x$$

An element $e \in X$ is called an **identity** for $\star$ if for every $x \in X$

$$e \star x = x \star e = x.$$

Given an element $x \in X$, if there exists an element $y \in X$ such that:

$$x \star y = y \star x = e,$$

then y is called the **inverse** of x with respect to the operation $\star$.

Remark 1. *Note that usual addition is an operation on the set of integers. It is associative, commutative. It has an identity and every element has an inverse.*
Observe that usual multiplication is an operation on the set of integers. It is associative, commutative. It has an identity but NOT every element has an inverse. Which integers admit an inverse with respect to multiplication?

Now we generalize the structure that integers have to the notion of a ring.

1.2 Rings

A **ring** $(R, +, \cdot)$ consists of a set R plus two operations:

addition: is an associative, commutative operation. There is an identity element denoted 0, and every element r has an additive inverse, denoted $-r$.

multiplication: is an associative, not necessarily commutative, operation. There is an identity element, denoted 1. It is not required for a nonzero element to have a multiplicative inverse.

Further, addition and multiplication must satisfy the distributive laws: for any three elements $r_1, r_2, r_3 \in R$:

D1:

$$(r_1 + r_2)r_3 = r_1r_3 + r_2r_3$$

D2:

$$r_3(r_1 + r_2) = r_3r_1 + r_3r_2$$

A **field** $(K, +, \cdot)$ is a ring where multiplication is commutative and every element different from 0 has a multiplicative inverse.

2 Examples

2.1 Rational numbers

The set of rational numbers $\mathbb{Q}$ with the usual operations of addition and multiplication is a field.

2.2 Polynomials

Let $\mathbb{R}[x]$ denote the set of polynomials in one variable with real coefficients. An element of $\mathbb{R}[x]$ is an expression of the form:

$$p(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0,$$

where all the a_i's are real numbers.

We define two operations as follows:

addition: if $p(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0, q(x) = b_nx^n + b_{n-1}x^{n-1} + \ldots + b_1x + b_0$, then

$$p(x)+q(x) := (a_n+b_n)x^n+(a_{n-1}+b_{n-1})x^{n-1}+\ldots+(a_1+b_1)x+(a_0+b_0)$$

multiplication: we define multiplication for special polynomials called monomials. If $p(x) = a_n x^n$ and $q(x) = b_m x^m$, then

$$p(x)q(x) = (a_n b_m)x^{n+m}$$

Question 1. *Give some thought to the following questions:*

1. *Can you define multiplication for arbitrary polynomials by imposing the distributive law?*
2. *Check that $\mathbb{R}[x]$ is a ring but not a field.*
3. *What are the elements of $\mathbb{R}[x]$ that admit a multiplicative inverse?*

2.3 Matrices

Let $M(2, \mathbb{R})$ be the set of 2×2 matrices with real entries. An element of $M(2, \mathbb{R})$ has the form:

$$A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$$

where all the a_{ij} are real numbers.

We define one addition and two multiplication operations as follows. if $A = \begin{bmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{bmatrix}$, and $B = \begin{bmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{bmatrix}$, then:

addition:

$$A + B := \begin{bmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{bmatrix},$$

multiplication 1:

$$A \star B := \begin{bmatrix} a_{11}b_{11} & a_{12}b_{12} \\ a_{21}b_{21} & a_{22}b_{22} \end{bmatrix},$$

multiplication 2:

$$AB := \begin{bmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{bmatrix},$$

Question 2. *Let us think about what we just defined:*

1. *Is $M(2, \mathbb{R})$ with addition and multiplication 1 a ring? Is it a field?*
2. *Is $M(2, \mathbb{R})$ with addition and multiplication 2 a ring? Is it a field?*
3. *What is the biggest difference you notice between the two ring structures?*
4. *In both cases, what are the elements that admit a multiplicative inverse?*

2.4 Functions

Let $\mathcal{C}([0,1])$ denote the set of real valued continuous functions from the closed interval $[0,1]$. An element of $\mathcal{C}([0,1])$ is denoted $f : [0,1] \to \mathbb{R}$, or by $f(x)$ or just f.

We define the operation of addition and multiplication of functions just like in calculus, by

$$f + g(x) := f(x) + g(x)$$

$$fg(x) := f(x)g(x)$$

Question 3. *Now for some questions on this example:*

1. *Is $\mathcal{C}([0,1])$ with the operation defined above a ring? Is it a field?*
2. *What elements in $\mathcal{C}([0,1])$ admit a multiplicative inverse?*
3. *How can we modify the set-up to obtain a field?*

2.5 $\mathbb{Z}/n\mathbb{Z}$

For every n, consider the set

$$\mathbb{Z}/n\mathbb{Z} := \{[0], [1], \ldots, [n-1]\}$$

Question 4. *Define an addition and a multiplication operations that are very similar to the usual operations on integers and make $\mathbb{Z}/n\mathbb{Z}$ into a ring.*

3 Functions of Rings

If we have two rings R_1 and R_2, then we are interested in studying the functions that "behave well", with respect to the operations. We formalize this concept with the following definition.

3.1 Homomorphism

A **homomorphism** of rings is a function

$$f : (R_1, +_1, \cdot_1) \to (R_2, +_2, \cdot_2)$$

such that for every $x, y \in R_1$:

- $$f(x_1 +_1 x_2) = f(x_1) +_2 f(x_2)$$
- $$f(x_1 \cdot_1 x_2) = f(x_1) \cdot_2 f(x_2)$$

A bijective ring homomorphism is called an **isomorphism**.

Question 5. *1. What constant function is always (and rather stupidly) a ring homomorphism?*

2. Show that the evaluation function at any point is a ring homomorphism. Define the evaluation as follows:

$$ev_7 : \mathbb{R}[x] \to \mathbb{R}$$

$$p(x) \mapsto p(7).$$

3. Is determinant a ring homomorphism from the ring of 2×2 matrices to $\mathbb{R}$?

Problem 1. *Consider the following rings:*

- $$(R_1, +_1, \cdot_1) = (\{0, 1\}, +, \cdot),$$

  where by definition we make $1 + 1 = 0$.

- $$(R_2, +_2, \cdot_2) = (\{-1, 1\}, \cdot, max).$$

Show that R_1 and R_2 are isomorphic.

3.2 Kernel of a homomorphism

Given a homomorphism of rings $f : (R_1, +_1, \cdot_1) \to (R_2, +_2, \cdot_2)$, the **kernel of f** consists of all elements $r \in R_1$ that are mapped to 0_2 by f:

$$Ker(f) := \{r \in R_1 \ s.t. \ f(r) = 0_2\}.$$

Note! The kernel of f is a subset of the initial ring R_1! Somehow this seems to be something people get confused about...

Question 6. *What is the kernel of the ring homomorphism $ev_0 : \mathcal{C}([0, 1]) \to \mathbb{R}$, defined by $ev_0(f) := f(0)$?*

3.3 Some basic theorems

Theorem 1. *Prove that in a ring R the additive identity and the multiplicative identity are unique.*

Theorem 2. *Let R be a ring, and denote by -1 the additive inverse of the multiplicative identity 1. Then show that for any other element $r \in R$, the additive inverse of r is $-1 \cdot r$. This justifies the common notation of denoting by $-r$ the additive inverse of r.*

Note: You actually need to use Theorem 5 to prove this one, so please use it . This theorem is not needed to prove Theorem 5, so there is no circular dependence introduced.

Theorem 3. *If* $f : (R_1, +_1, \cdot_1) \to (R_2, +_2, \cdot_2)$ *is a ring homomorphism, then*

$$f(0_1) = 0_2$$

Theorem 4. *If* $f : (R_1, +_1, \cdot_1) \to (R_2, +_2, \cdot_2)$ *is a ring homomorphism, then*

$$f(-r) = -f(r)$$

4 Group-Work

4.1 Zero Divisors

Theorem 5. *If* R *is a ring, for any* $r \in R$

$$0 \cdot r = r \cdot 0 = 0$$

This is a familiar statement, even if we had to be a bit pickier in how to prove it. For "ordinary" numbers the converse statement is also true:

Statement 1. *If* x *and* y *are such that* $xy = 0$*, then either* $x = 0$ *or* $y = 0$*.*

Problem 2. *Show that Statement 1 does not need to be true for arbitrary rings. Go through our examples in Section 2 and decide if Statement 1 fails or holds for each of those rings.*

An element $r \in R$ such that $r \neq 0$ but such that there exist $s \neq 0 \in R$ with $rs = 0$ is called a **zero divisor**.

Problem 3. *Prove that if* $r_1 \in R_1$ *is a zero divisor and* $f : (R_1, +_1, \cdot_1) \to (R_2, +_2, \cdot_2)$ *is an* ***injective*** *ring homomorphism, then* $f(r_1)$ *is also a zero divisor (in* R_2*, of course).*

Show that the converse statement needs not be true: you can have an $r_1 \in R_1$ *NOT a zero divisor and a ring homomorphism* f *such that* $f(r_1)$ *is a zero divisor.*

As a challenge, see if you can construct a non-injective ring homomorphism where r *is a zero-divisor and* $f(r)$ *isn't. (Hint: think of* R *as matrices but with the silly multiplication component by component. Then what elements are* 0*-divisors? Can you think of a nontrivial ring homomorphism to* $\mathbb{R}$*?)*

Problem 4. *Is the sum of two zero divisors a zero divisor?*

4.2 Ideals

It turns out that the notion of "subring" is not actually very well behaved. The more interesting notion of *subsets of a ring that we want to care about* is played by things called ideals.
Note: just to keep things a little simpler, in this section we assume the multiplication to be commutative.

We define an **ideal** of R to be a subset $I \subset R$ of elements closed under addition and closed under multiplication by an arbitrary element of R. More in detail, $I \subset R$ is an ideal if:

- for every $i_1, i_2 \in I$, the element $i_1 + i_2 \in I$.
- for every $i \in I$, and for every $r \in R$, the element $i \cdot r \in I$.

Problem 5. *What are the two silliest ideals that you can think of? Can you give me some example of ideals in* $\mathbb{Z}$ *?*

Problem 6. *Suppose* I *is an ideal of* $\mathbb{Z}$ *such that* I *contains two coprime numbers. What is* I*? Why?*

Problem 7. *What are the ideals of a field* K*?*

Problem 8. *Given a ring homomorphism* $f : (R_1, +_1, \cdot_1) \to (R_2, +_2, \cdot_2)$ *show that* $Ker(f)$ *is an ideal of* R_1*.*

4.3 Quotient Rings

Again, to keep things a little bit simple, let us restrict our attention to rings where multiplication is commutative.

Suppose you have an equivalence relation $\sim$ on a ring R. Then we get a quotient set $R/\sim$. We want to understand when we can naturally make this quotient set into a ring.

Define an equivalence relation to be **good** (or compatible with addition and multiplication) if, given four elements $r_1, r_2, s_1, s_2 \in R$ such that $r_1 \sim r_2$ and $s_1 \sim s_2$, then :

1. $$r_1 + s_1 \sim r_2 + s_2$$
2. $$r_1 \cdot s_1 \sim r_2 \cdot s_2$$

If $\sim$ is a good equivalence relation, the addition and multiplication on the quotient set

$$[r_1] \boxplus [r_2] = [r_1 + r_2]$$

$$[r_1] \boxdot [r_2] = [r_1 \cdot r_2]$$

are well defined and turn the quotient set into a ring called the **quotient ring**.

Problem 9. *Show that $\mathbb{Z}/n\mathbb{Z}$ is a quotient ring.*

Problem 10. *Given a good equivalence relation on a ring R, show that the projection function*

$$p : R \to R/\sim$$
$$r \mapsto [r]$$

is a ring homomorphism.

Problem 11. *Show that given a good equivalence relation, the equivalence class of 0 ($[0]$ thought of as a subset of R rather than one element of the quotient ring) is an ideal in R. Viceversa, show that given an ideal of R, you can always define a good equivalence relation on R. In that case the quotient ring is often denoted R/I.*

4.4 Challenge: what is This?

Define the following equivalence relation on the set of polynomials $\mathbb{R}[x]$:

$$p(x) \sim q(x) \text{ if } \ x^2 + 1 \text{ divides } q(x) - p(x)$$

1. Check that this equivalence relation is a good equivalence relation on polynomials.
2. Write down some polynomials that live in the equivalence class of 0, of 1 and of -1.
3. Does this quotient remind you of something? Can you find a ring (or field) isomorphism with some familiar ring (or field)?