De l'arithmétique ailleurs que sur $\mathbb{Z}$

Bashar Dudin

Abstract

This tutoring sheet aims at giving you a feeling for what a ring is, the different types of rings you could meet and their interconnections. It does also invite you into a new world where you'll be working with a number of rings that happen to be of interest for computer science.

Contents

1 Looking for Rings

Within this section you'll be learning how to decide on whether standard sets and their subsets come with a natural ring structure. You'll also be navigating the different properties of rings and checking for some of theses properties in practical cases.

Exercise 1-1 Consider the list of sets, each endowed with two internal laws:

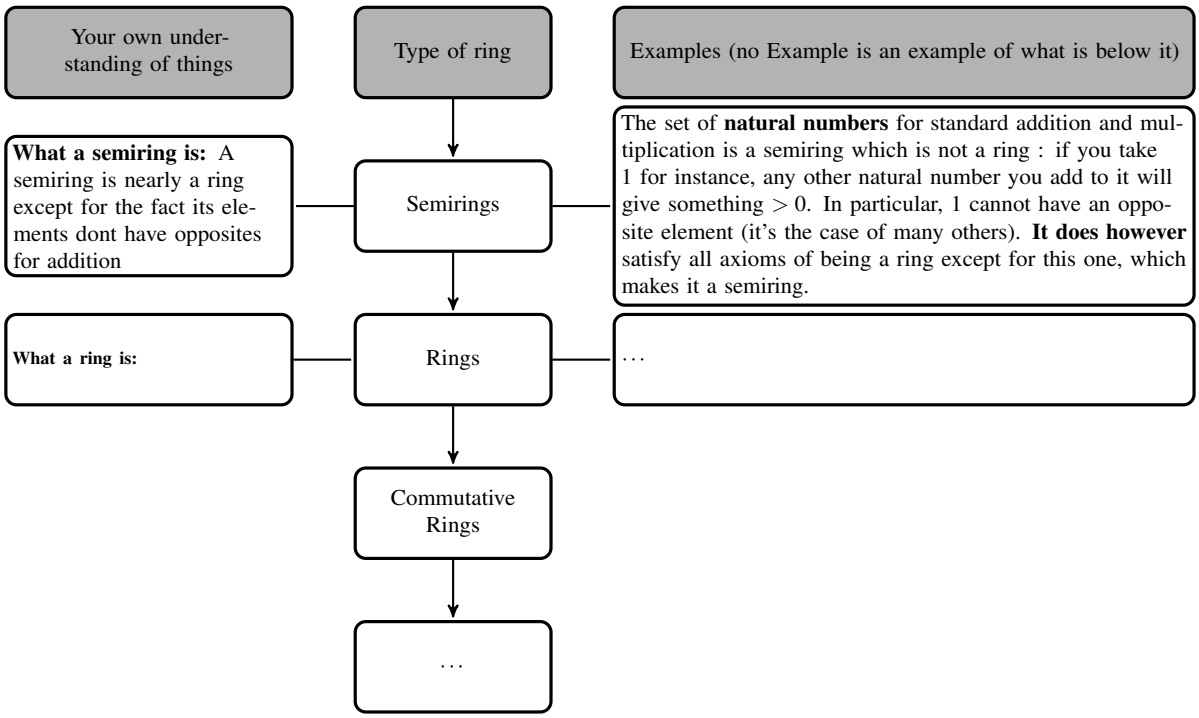
- $(\mathbb{N}, +, \times)$
- $(\mathbb{Z}/5\mathbb{Z}, +, \times)$
- $(\mathbb{Z}/6\mathbb{Z}, +, \times)$
- $(\mathbb{Q}, +, \times)$
- $(\mathbb{Z}[X], +, \times)$
- $(\mathbb{Q}(X), +, \times)$

- $(\mathbb{N}^{\mathbb{N}}, +, \times)$
- $(\mathscr{M}_5(\mathbb{R}), +, \times)$ (square matrices of size 5 with matrix multiplication)
- $(\mathscr{M}_5(\mathbb{R}), +, \cdot)$ (square matrices of size 5 with pointwise multiplication)
- $(S, +, \times)$ where S is the set of convergent sequences
- $(E, +, \times)$ where E is the set of convergent sequences having limit 0
- $(\mathbb{R}^{\mathbb{R}}, +, \times)$
- $(\mathbb{R}^{\mathbb{Q}}, +, \circ)$

1. Which elements of the list are not rings? Justify your answer.
2. Identify neutral elements of the structures excluded by the first question and discuss ring axioms that are not evidently satisfied.
3. Group graphically the rings of the list considering the following properties:
   - commutativity
   - integrity
   - being a field
   - having no non-zero divisors
   - being finite.

   In each case justify your answer.

Exercise 1-2 The activity you're having here aims at building a mindmap of the different types of structures we've been looking at in this course. You're expected to complete the following mindmap (you're allowed to get the help of Google!). You're invited to first work out the assignment individualy then collaboratively.



2 Quotients of Polynomial Rings

This section is devoted to you being able to extend the quotient construction you've encountered for $\mathbb{Z}/n\mathbb{Z}$ to the case of polynomial rings and build simple cases of finite fields that are not cyclic for addition.

Exercise 2-3 Denote by $\mathscr{Q}_{X^2-1}$, $\mathscr{Q}_{X^2-3}$ the quotient rings of $\mathbb{Q}[X]$ by X^2-1 and X^2-3.

1. Check whether $\mathscr{Q}_{X^2-1}$ and $\mathscr{Q}_{X^2-3}$ are integral domains: if not describe the set of zero divisors, otherwise prove your statement.
2. What is the inverse of X^2 in both $\mathscr{Q}_{X^2-1}$ and $\mathscr{Q}_{X^2-3}$?
3. Is any of $\mathscr{Q}_{X^2-1}$ or $\mathscr{Q}_{X^2-3}$ a field? Justify your answer.

Exercise 2-4

1. Can one have finite fields of any order?
2. Write down the tables for addition and multiplication of a finite field having 8 elements.
3. Describe a quotient of $\mathbb{F}_3[X]$ giving you a field have order 9. How many operations would you actually need to compute if you had to write down the addition and multiplication tables of such a field?

3 Arithmetic over Integer Rings

In this section you'll be working out arithmetic questions in a ring which is not $\mathbb{Z}$.

Exercise 3-5 We're interested in the arithmetic of the ring $(\mathbb{Z}[i],+,\times)$ where addition and multiplication are the ones of complex numbers. The set $\mathbb{Z}[i]$ is given by

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

1. Give examples of prime numbers in $\mathbb{Z}$ that are not irreducible in $\mathbb{Z}[i]$.
2. The norm of an element $x = a+ib$ is given by

   $$N(x) = a^2+b^2.$$

   Give all invertible elements in $\mathbb{Z}[i]$.
3. Give a necessary and sufficient condition on a prime number p, in terms of N, for it not to be irreducible in $\mathbb{Z}[i]$.
4. The ring $\mathbb{Z}[i]$ is euclidean for the norm N, thus a unique factorization domain. Are all the $\mathbb{Z}[i\sqrt{d}]$ for prime d factorial domains?

Exercise 3-6 We're interested in the arithmetic of the ring $(\mathbb{Z}[\sqrt{2}],+,\times)$ where addition and multiplication is the one you have on real numbers. The set $\mathbb{Z}[\sqrt{2}]$ is given by

$$\mathbb{Z}[\sqrt{2}] = \left\{a+b\sqrt{2} \mid a,b \in \mathbb{Z}\right\}.$$

1. Give examples of prime numbers in $\mathbb{Z}$ that are not irreducible in $\mathbb{Z}[\sqrt{2}]$.

2. The norm of an element $x = a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ is given by

$$N(x) = a^2 - 2b^2.$$

   Describe invertibles of $\mathbb{Z}[\sqrt{2}]$ using N. Does $\mathbb{Z}[\sqrt{2}]$ seem to be finite?

3. Give a sufficient and necessary condition on p, using N, not to be irreducible in $\mathbb{Z}[\sqrt{2}]$.