Rings

Definition and Summary

Prof Hans Georg Schaathun

Høgskolen i Ålesund

Autumn 2013 – Video 3/1
Recorded: September 30, 2013

The four arithmetic operations

- We have studied $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$
- Usual arithmetic operations
  - Addition and Multiplication
- We have mentioned that $\mathbb{Z}_n$ is a ring.

Definition

- A set R, with operations $+$ and $\cdot$ is called a ring if the following axioms hold

1. $(x + y) + z = x + (y + z)$ (associtativity of addition)
2. $x + y = y + x$ (commutativity of addition)
3. There is an element $0 \in R$ such that $x + 0 = x$ for all $x \in R$
4. For any $x \in R$ there is an element $(-x) \in R$, such that $x + (-x) = 0$.
5. There is an element 1 such that $x \cdot 1 = 1 \cdot x = x$ for all $x \in R$
6. $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ (associtativity of multiplication)
7. $x \cdot y = y \cdot x$ (commutativity of multiplication)
8. $x \cdot (y + z) = x \cdot y + x \cdot z$ (distributive law)

What the ring is missing

- We cannot divide in general
- The inverse x^{-1} is defined such that $x \cdot x^{-1} = 1$
  - may exist for some x and not for others
- When $1/x = x^{-1}$ is defined,
  - $y/x = y \cdot x^{-1}$ (by definition)

The inverse

- An element x is either
  - zero divisor
  - invertible
- Either there is
  - y such that $x \cdot y = 0$, or
  - y such that $x \cdot y = 1$
- In a modular ring $\mathbb{Z}_n$
  - $k > 1$ divides x and n: zero divisor
  - Otherwise: invertible

Example

Exercise

Which are the zero divisors in $\mathbb{Z}_6$?

Exercise

Consider the English alphabet $\mathbb{Z}_{26}$ *and the Scandinavian one* $\mathbb{Z}_{29}$*. What are the zero elements in each of the rings?*