Lecture Mon 9/12/05

Algebra Definitions 1

We define some terms concerning generalized number systems.

- A **ring** is a set R along with operations of addition $+ : R \times R \to R$ and multiplication $\bullet : R \times R \to R$, satisfying the following properties:

  (i) $+$ associativity: $(a+b)+c = a+(b+c)$ for all $a, b, c \in R$.

  (ii) $+$ identity: there exists $0 \in R$ such that $0 + a = a + 0 = a$ for all $a \in R$.

  (iii) $+$ inverse: for any $a \in R$, there is a $b \in R$ with $a + b = b + a = 0$: we denote b by $-a$.

  (iv) $+$ commutativity: $a + b = b + a$ for all $a, b \in R$.

  (i′) $\bullet$ associativity: $(a \bullet b) \bullet c = a \bullet (b \bullet c)$ for all $a, b, c \in R$.

  (ii′) $\bullet$ identity: there exists $1 \in R$ such that $1 \bullet a = a \bullet 1 = a$ for all $a \in R$.

  (v) distributivity: $a \bullet (b + c) = a \bullet b + a \bullet c$ and $(a + b) \bullet c = a \bullet c + b \bullet c$.

- A **division ring** is a ring satisfying:

  (iii′) $\bullet$ inverse: for any non-zero $a \in R$, there is a $b \in R$ with $a \bullet b = b \bullet a = 0$: we denote b by a^{-1} or $1/a$.

- A **commutative ring** is a ring satisfying:

  (iv′) $\bullet$ commutativity: $a \bullet b = b \bullet a$ for all $a, b \in R$.

- A **field** is a ring satisfying both (iii′) and (iv′).

- A **unit** in ring R is an element a which has a mulitiplicative inverse $a^{-1} \in R$. The set of units is denoted $R^{\times}$. Thus, a field F is a ring in which every non-zero element is a unit: $F^{\times} = F \setminus \{0\}$. Elements of a ring are **associates** if they differ by a unit factor: $a, b \in R$ such that $a = ub$ for $u \in R^{\times}$.

- A **zero-divisor** in a ring R is an element $a \neq 0$ such that $a \bullet b = 0$ for some $b \in R$. A **domain** is a commutative ring with no zero-divisors.

- A **Euclidean ring** is a domain R along with a function

  $$\text{size} : R \setminus \{0\} \to \mathbb{N}$$

  (where $\mathbb{N} = \{0, 1, 2, \cdots\}$) such that for any $a, b \in R$, there are $q, r \in R$ with $a = qb + r$ and $r = 0$ or $\text{size}(r) < \text{size}(b)$. The elements q, r are not necessarily unique.

Examples

- $\mathbb{Z}$, the integers, is commutative ring, a Euclidean domain, but not a field. The units are: $\mathbb{Z}^\times = \{\pm 1\}$.
- $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, the rational, real and complex numbers, are all fields.
- $\mathbb{Z}_n$, clock arithmetic mod n, is a commutative ring for any n. It is a field for $n = 2$. For which n is it a field? What are the units and zero-divisors?
- $M_n(\mathbb{Q})$, the $n \times n$ matrices with entries in $\mathbb{Q}$ under matrix addition and multiplication, is a ring, but not commutative, and without division. The units are the nonsingular matrices, the zero-divisors are the singular matrices (prove!).
- $\mathbb{Q}[x]$, the polynomial functions:

  $$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n ,$$

  with $a_0, \ldots, a_n \in \mathbb{Q}$, under the pointwise addition and multiplication, is a commutative ring and a domain. The units are the non-zero contstant functions $f(x) = c$. It is also a Euclidean domain under the polynomial division algorithm, with size function $\operatorname{size} f(x) = \deg f(x) = n$, the degree of the highest non-zero term $a_n x^n$.

  All of these features make the polynomial ring $\mathbb{Q}[x]$ analogous to the integer ring $\mathbb{Z}$.
- $\mathbb{Q}(x)$, the rational functions, is the set of quotients of two polynomial functions: $f(x)/g(x)$ with $g(x) \neq 0$. This is a field, analogous to $\mathbb{Q}$.