AM 106/206: Applied Algebra          Prof. Salil Vadhan

Lecture Notes 13

October 25, 2010

- Reading: Gallian Chs. 12 & 13

# 1  Rings

- Many common algebraic structures have not just one, but two operations ("addition" and "multiplication") that are related to each other. In the rest of the course, we will study common properties that such pairs of operations have and general phenomena that follow from these properties, and use this theory to understand specific algebraic structures that are useful in applications.

- **Def:** $R$ with two binary operations $+, \cdot$ is a *ring* if it has the following properties:

  1. $(R, +)$ is an abelian group.
  2. $\cdot$ is associativite.
  3. Distributive Law: $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(a + b) \cdot c = a \cdot c + b \cdot c$ for all $a, b, c \in R$.

- **Additional Properties:**

  - *Commutative Rings:* $ab = ba$ for all $a, b \in R$
  - *Rings with Unity:* $\exists 1 \in R \setminus \{0\}$ such that $1a = a1 = a$ for all $a \in R$.
  - *Integral Domain:* Commutative ring with unity in which there are no *zero divisors*: if $a$ and $b$ are nonzero, then $ab$ is nonzero. (Equivalently, the ring allows cancellation: $ab = ac \Rightarrow b = c$.)
  - *Fields:* Commutative ring with unity in which every nonzero element has a multiplicative inverse.
  - **Q:** what is the relation between integral domains and fields?

- **Venn Diagram of Properties:**




- **Notation:**

  - $0 =$ additive identity, $1 =$ multiplicative identity (if it exists)
  - $-a =$ additive inverse, $a^{-1} =$ multiplicative inverse (if it exists)
  - $na = a + a + \cdots + a$ for $n \in \mathbb{N}$

| Set/notation | Addition | Multiplication | Ring? | Commut.? | Unity? | Int. Domain? | Field? |
|---|---|---|---|---|---|---|---|
| $\mathbb{Z}$ | standard | standard | | | | | |
| $\mathbb{C}, \mathbb{Q}, \mathbb{R}$ | standard | standard | | | | | |
| $\mathbb{Z}_n$ | $+ \bmod n$ | $\cdot \bmod n$ | | | | | |
| $\mathbb{Q}[x] = \{\text{polys with rational coeffs}\}$ | standard | standard | | | | | |
| $\mathbb{Q}^{\leq d}[x] = \text{polys of degree} \leq d$ | standard | standard | | | | | |
| $M_n(\mathbb{R})$ | componentwise | matrix mult | | | | | |
| subsets of $\{1, \ldots, 100\}$ | $\cup$ | $\cap$ | | | | | |
| $L_2(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R} \mid \int |f|^2 < \infty\}$ | standard | $(f * g)(x) = \int_t f(t)g(x-t)dt$ | | | | | |
| $R_1 \times R_2$, $R_1, R_2$ rings | componentwise | componentwise | | | | | |
| $R[x] = \{\text{polys with coeffs from } R\}$ | standard | standard | | | | | |
| $\{0\}$ | | | | | | | |
| $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ | standard | standard | | | | | |
| $\mathbb{Q}[i] = \{a + bi : a, b \in \mathbb{Q}\}$ | standard | standard | | | | | |
| $\mathbb{Z}_3[i] = \{a + bi : a, b \in \mathbb{Z}_3\}$ | standard | standard | | | | | |