Dillan Marroquin
MATH 331.1001
Scribing Week 11
Due. 8 November 2021

Lecture 26

Paulin Chapter 4: Rings!

Idea: Study objects like $(\mathbb{Z}, +, 0, *, 1)$, develop an abstract notion of primes and the fundamental theorem of arithmetic.

Definition (26.1)**.** A <u>**ring**</u> $(\mathbf{R}, +, \mathbf{0}, *, \mathbf{1})$ is a set R equipped with binary operators $+, * : R \times R \to R$ and elements $0, 1 \in R$ such that

1. $(R, +, 0)$ is an abelian group,
2. $(R, *, 1)$ is a monoid (i.e. a group where multiplicative inverses may not exist),
3. Left/Right distributive law holds: $\forall a, b, c \in R$, $(a+b)*c = a*c + b*c$ and $a*(b+c) = a*b + a*c$.

<u>**Notation:**</u> $ab := a*b$ and $\forall n \geq 0 \in Z$, $na := a + a \cdots + a$ (n times) and $a^n := a*a*\cdots*a$ (n times). Note that $na \neq a^n$ in general.

Definition (26.2)**.** A ring R is commutative iff $\forall a, b \in R$, $a*b = b*a$.

Basic Examples of Rings

1. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Commutative.
2. $(\mathbb{Z}/n, \overline{+}, \overline{0}, \overline{*}, \overline{1})$. Commutative.
3. The Zero Ring $R = \{0_R\}$, where $1_R = 0_R$. Commutative.
4. $M_n(\mathbb{R}) := \{n \times n$ matrices with entries in $\mathbb{R}\}$, $(M_n(\mathbb{R}), +, 0_n, *, I_n)$. Non-commutative for $n \geq 2$.
5. $\mathcal{C}([0,1]) := \{f : [0,1] \to \mathbb{R} | f$ is continuous$\}$. In this ring, $(f+g)(x) := f(x) + g(x)$, $(fg)(x) := f(x)g(x)$, $0(x) := 0 \in \mathbb{R}$, $1(x) := 1 \in \mathbb{R}$ $\forall x \in [0,1]$.

Abstract Properties of Rings

Proposition (26.3)**.** Let R be a ring.

1. $\forall n, m \geq 1$, let $a_1, \ldots, a_n \in R$ and $b_1, \ldots, b_m \in R$. Then $\left(\sum_{i=1}^n a_i\right) \cdot \left(\sum_{j=1}^m b_j\right) = \sum_{i=1}^n \sum_{j=1}^m a_i b_j$.
2. $\forall a \in R$, $a*0 = 0 = 0*a$.
3. $\forall a, b \in R$, $a(-b) = -a(b) = -ab$, where $-b, -a$ are the additive inverses of b, a respectively. In particular, $(-a)(-b) = ab$.

Important Example: Polynomial Rings

Let R be a commutative ring. Then

$$R[x] := \{a_0 + a_1 x + a_2 x^2 + \cdots + a_{n-1} x^{n-1} + a_n x^n | \forall n \geq 0 \ a_i \in R\} = \text{"}R \text{ adjoin } x\text{"}.$$

Let $f, g \in R[x]$. Write $f = \sum_{i=0}^n a_i x^i$, $g = \sum_{j=0}^m b_j x^j$. WLOG, assume $m \leq n$. Define $b_{m+1} = b_{m+2} = \cdots = b_n = 0 \in R$, then $f + g := \sum_{i=0}^n (a_i + b_i) x^i$. Also, $fg := \sum_{k=0}^{m+n} c_k x^k$, where $c_k := \sum_{l=0}^k a_l b_{k-l}$.

Lecture 27

Additive Identity: $0 := \sum_i a_i x^i$, $a_i = o \in R\ \forall i \geq 0$.

Multiplicative Identity: $1 := \sum_i a_i x^i$, $a_o = 1 \in R$, $a_i = 0 \in R\ \forall i \geq 1$.

Proposition (27.1)**.** R commutative implies $R[x]$ is commutative.

Remark. $R[x][y]$. This is just a polynomial in 2 variables.

Definition (27.2)**.** Let $f = \sum a_k x^k \in R[x]$, where $\sum a_k x^k$. Then the **degree** of f, $\deg(f) \in \mathbb{N}$ is the largest $n \in \mathbb{Z}$ such that $a_n \neq 0$. Often, $\deg(0) := -\infty$.

Basic Constructions

Definition (27.3)**.** Let R be a ring. A subset $S \subseteq R$ is a **subring** iff

1. $(S, +, 0_R) \leq (R, +, 0_R)$ is a subgroup with respect to $+$.
2. $\forall x, y \in S$, $x * y \in S$. i.e. S is closed under multiplication.
3. $1_R \in S$.

We write $S \leq R$ to denote that S is a subring of R.

Example.

1. We have $\mathbb{Z} \leq \mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$.
2. Let R be commutative. Then $R \leq R[x]$.
3. (Non-Commutative Examples): Let $R = M_2(\mathbb{R})$ and $S = \left\{A \in R | A = \alpha = \begin{pmatrix} a_1 & a_2 \\ 0 & 3 \end{pmatrix}\right\}$. Then $S \leq R$.

CAUTION!!! Some authors...

1. don't require a ring to have 1 (multiplicative identity)
2. don't require subrings to have $1_R \in S$ (no Axiom 3).

Basic Constructions

1. $n\mathbb{Z} \not\leq \mathbb{Z}$, $n > 1$ since $1 \notin \mathbb{Z}$.
2. If $R \neq \{0_R\}$, then $\{0_R\} \not\leq R$ since $1_R \notin \{0_R\}$.
3. Take $S = \{f = \sum a_i x^2 \in R[x] | a_0 = 0\} \not\leq R[x]$ since $1 \notin R[x]$.

Lecture 28

Ring Homomorphisms

Definition (28.1)**.** Let R, S be rings. A **ring homomorphism** from R to S is a function $\varphi : R \to S$ such that $\forall a, b \in R$,

1. $\varphi(a + b) = \varphi(a) + \varphi(b)$,
2. $\varphi(ab) = \varphi(a)\varphi(b)$, and
3. $\varphi(1_R) = 1_S$. A **ring isomorphism** is a ring homomorphism φ such that φ is a bijection.

Example.

1. $\mathrm{id} : R \to R$ is a ring isomorphism. BOOOORING!!!
2. Let $n > 1$. Then $\pi : \mathbb{Z} \to \mathbb{Z}/n$, $\pi(a) := [a]$ is a ring homomorphism.
3. (NON-EXAMPLE) Let $\det : M_2(\mathbb{R}) \to \mathbb{R}$ be a function. Then Axioms 2 and 3 are satisfied, but not Axiom 1 since $\det(A + B) \neq \det(A) + \det(B)$ in general.

Proposition (28.2)**.** Let $r \in R$. The function $\mathrm{ev}_r(f) := f(r)$ is a ring homomorphism ("evaluation at r").

In general, elements of $R[x]$ "aren't functions."

Example. $\mathbb{Z}/2[x]$.

$$\begin{aligned} \deg(-\infty) &: \overline{0} & \qquad \deg(1) &: x, x+\overline{1} \\ \deg(0) &: \overline{1} & \qquad \deg(2) &: x^2, x^2+x, x^2+\overline{1}, x^2+x+\overline{1}. \end{aligned}$$

The number of ev homomorphisms is 2: $\mathrm{ev}_{\overline{0}}, \mathrm{ev}_{\overline{1}} : \mathbb{Z}/2[x] \to \mathbb{Z}/2$.

Let $f := x^2 + x + \overline{1}$, $g := \overline{1}$. Then $\mathrm{ev}_{\overline{0}}(f) = \overline{1}$, $\mathrm{ev}_{\overline{1}}(f) = \overline{1}^2 + \overline{1} + \overline{1} = \overline{1}$.
Also, $\mathrm{ev}_{\overline{0}}(g) = \overline{1}$, $\mathrm{ev}_{\overline{1}}(g) = \overline{1}$, BUT $f \neq g$.

Definition (28.3)**.** Let $\varphi : R \to S$ be a ring homomorphism. The <u>**kernel**</u> of φ is the subset $\ker(\varphi) := \{r \in R | \varphi(r) = 0_S\}$ of R.
The <u>**image**</u> of φ is the subset $\mathrm{im}(\varphi) := \{\varphi(r) | r \in R\}$ of S.

Proposition (28.4)**.**

1. $\mathrm{im}(\varphi) \leq S$ is a subgroup of S.
2. $\ker(\varphi) \leq R$ is a subring of R iff $S = \{0_S\}$ is the trivial ring.