Dillan Marroquin
MATH 331.1001
Scribing Week 13
Due. 22 November 2021

Lecture 32

Properties of Elements in Rings

Recall from Lecture 6 the following:

Theorem (6.2)**.** $(\mathbb{Z}/n^\times, *, [0])$, where $\mathbb{Z}/n^\times := \{[k] \in \mathbb{Z}/n - \{[0]\} | \gcd(k, n) = 1\}$ for $n > 1$ is a group.

Example. We have $Z/4^\times = \{[1], [3]\}$. Here, $[1] * [1] = [1]$ and $[3] * [3] = [8] = [1]$. Therefore, every element has a multiplicative inverse. Also, if you have $[a], [b] \in \mathbb{Z}/4$ such that $[a] * [b] = [0]$, then $[a], [b]$ need not be $[0]$: $[2] * [2] = [4] = [0]$. On the other hand, if $n = p$ prime, then $(\mathbb{Z}/p^\times) = \mathbb{Z}/p - \{[0]\}$. Every non-zero element of $\mathbb{Z}/p$ has a multiplicative inverse.

Definition (32.1)**.** Let R be a ring. An element $a \in R$ is a **unit** iff it has a multiplicative inverse. i.e. $\exists u \in R$ such that $au = ua = 1_R$. Define $R^\times := \{a \in R | a \text{ is a unit}\}$.

Proposition (32.2)**.** Let $(R, +, 0_R, *, 1_R)$ be a ring. Then...

1. $(R^\times, *, 1_R)$ is a group.
2. If $a \in R^\times$, its inverse is unique.
3. If $1_R \neq 0_R$, $0_R \notin R^\times$.

Proof. 1. Definition of a ring implies $(R, *, 1_R)$ is a monoid. This implies $*$ is associative and 1_R is the identity element. Now we need to show $R^\times$ is closed with respect to $*$. Let $a, b \in R^\times$, and let u, w be the inverses, respectively. WTS $a * b \in R^\times$. We have $a * u = 1_R = u * a$ and $b * w = 1_R = w * a$. Now consider $(w * u) * (a * b) = w * (u * a) * b = w * 1_R * b = w * b = 1_R$. So $(a * b) * (w * u) = a * (b * w) * u = a * 1_R * u = a * u = 1_R$. Therefore $a * b \in R^\times$.

2. By 1. above, $R^\times$ is a group which implies that the inverse of any element in the group is unique.
3. Use the contrapositive. Suppose $0_R \in R^\times$. By definition, $\exists u \in R$ such that $0_R u = 1_R$. Thus, $0_R u = 0_R$ by 26.3.

∎

Definition (32.3)**.** A ring R is a **division ring** iff $R^\times = R - \{0_R\}$. A **field** is a commutative division ring. Fields are denoted $\mathbb{K}$.

Examples of fields: $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p := \mathbb{Z}/p$.

Another example: $\mathbb{K}(x) := \left\{ \frac{p(x)}{q(x)} \middle| p, q \in \mathbb{K}[x],\ q \neq 0 \right\}$. These are rational functions in 1 variable.

Lecture 33

Example (A division ring, but not a field)**.** The quarternions: $\mathbb{H} := \{a + ib + jc + kd | a, b, c, d \in \mathbb{R}\}$, where $i * i = j * j = k * k = -1 \in \mathbb{R}$, $i * j = k$, $j * i = -k$ (non-commutative). If $q = a + ib + jc + kd$, then $\overline{q} := a - ib - jc - kd$ is the conjugate of q and $q * \overline{q} = a^2 + b^2 + c^2 + d^2$.
For $q \neq 0 \in \mathbb{H}$, $q^{-1} q = q q^{-1} = 1$, $q^{-1} = \frac{\overline{q}}{q\overline{q}}$.
Subrings: $\mathbb{R} \leq \mathbb{C} \leq \mathbb{H}$. Group of Units: $\mathbb{R}^\times \leq \mathbb{C}^\times \leq \mathbb{H}^\times$ subgroups. "Norm 1 integer units": $\{\pm 1\} \leq \{\pm 1, \pm i\} \leq \{\pm 1, \pm i, \pm j, \pm k\}$.

Definition (33.1)**.** Let $R \neq 0$ be a ring. An element $a \neq 0 \in R$ is a **zero divisor** if $\exists b \neq 0$ such that $ab = 0$ or $ba = 0$.

Example. 1. $[3] \in \mathbb{Z}/6$ is a zero divisor since $[3] \cdot [2] = [6] = [0]$, but $[3] \neq [0]$, $[2] \neq [0]$.

2. Let R be a non-trivial ring: $R \times R$. Then an element $(1, 0) \cdot (0, 1) = (0, 0)$ is a zero divisor.

3. For the integers $\mathbb{Z}$, there exists no such zero divisor.

Definition (33.2)**.** A ring R is an **integral domain** iff

1. $R \neq 0$
2. R is commutative
3. R has no zero divisors

Proposition (33.3)**.** A field $\mathbb{K}$ is an integral domain.

Remark. An **entire ring** as defined in Paulin's notes is a ring $R \neq 0$ that has no zero divisors.

Polynomial Rings and Zero Divisors

Suppose $f, g \in \mathbb{R}[x] - \{0\}$. Then $\deg(f) = m$, $\deg(g) = n$, and $\deg(fg) = m + n$.
On the other hand, $f = [3]x^3$, $g = [2]x^2 + x \in \mathbb{Z}6[x]$. So $\deg(f) = 3$, $\deg(g) = 2$, and $\deg(fg) = [3]x^4 < \deg(f) + \deg(g)$.

Theorem (33.4)**.** Let R be an integral domain. Then...

1. If $f, g \in R[x] - \{0_R\}$, then $\deg(fg) = \deg(f) + \deg(g)$.
2. $\mathbb{R}[x]$ is an integral domain.

Lecture 34

Proof (Thm 33.4).

1. Let $\deg f = n \geq 0$, $\deg g = m \geq 0$. Then $f = \sum_{i=0}^{n} a_i x^i$, $g = \sum_{j=0}^{m} b_j x^j$ for a_i, $b_j \in R$. By definition of degree, $a_n \neq 0$ and $b_m \neq 0$. Consider $fg = a_n b_m x^{n+m} + (a_n b_{m-1} + a_{n-1} b_m) x^{n+m-1} + \cdots + a_0 b_0$. Note that $a_n b_m \neq 0$ since R is an integral domain and $a_n \neq 0$, $b_n \neq 0$. So $\deg fg = n + m = \deg f + \deg g$.
2. Let f, $g \in R[x] - \{0\}$. WTS $fg \neq 0$. Therefore $\deg f = n \geq 0$, $\deg g = m \geq 0$. Therefore as in 1. above, we have $fg = a_n b_m x^{n+m} + \cdots$ with $a_n \neq 0$ and $b_m \neq 0$. Thus $a_n b_m x^{n+m} \neq 0$ implies $fg \neq 0$.

■

Corollary (34.1)**.** If $\mathbb{K}$ is a field, then $\mathbb{K}(x)$ is an integral domain.

Remark. If R is an integral domain and we have $ac = bc$ in R with $c \neq 0$, then $a = b$.

Principal and Prime Ideals in Commutative Rings

From here on, R is assumed to be a non-trivial commutative ring (so $0_r \neq 1_r$).

Proposition (34.2)**.** Let $a \in R$. The subset $(a) := \{ra | r \in R\} \subseteq R$ is an ideal called the **principal ideal** generated by a.

Example. We have $n\mathbb{Z} = (n)$ when $R = \mathbb{Z}$.

Definition (34.3)**.** An ideal $I \trianglelefteq R$ is **principal** iff $\exists a \in I$ such that $I = (a)$.

Theorem (34.4)**.** Every ideal in $\mathbb{Z}$ is principal.

Proof. Suppose $I \trianglelefteq \mathbb{Z}$ is an ideal. By definition of ideal, $(I, +, 0) \leq (\mathbb{Z}, +, 0)$ is a subgroup. Recall $\mathbb{Z}$ is a cyclic (additive) group. In particular, $\mathbb{Z} = \langle 1 \rangle$. Theorem 13.3 says every subgroup of a cyclic group is cyclic. Therefore $\exists n \in I$ such that $I = \langle n \rangle = n\mathbb{Z}$. As an ideal, $n\mathbb{Z} = (n)$. ■