MATH 3022 Algebra II **Lecture 3**

LECTURE JOE TRAN

Recall: An *integral domain* is a commutative ring with identity that has no zero divisors. For example, $\mathbb{Z}$, $\mathbb{F}$[1], $\mathbb{Z}_p$ are integral domains. Observe that if we let D be an integral domain, and $a, b \in D$. If $ab = 0$, then either $a = 0$ or $b = 0$.

We will come back to talk about the set $R[x]$, where R is one of $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{Z}_p$.

Proposition 1 (Cancellation Law)**.** *Let D be a commutative ring with identity. Then D is an integral domain if and only if for every nonzero $d \in D$ with $da = db$, then $a = b$.*

Proof. ($\Rightarrow$) Assume that D is an integral domain, and assume that $da = db$ with $d \neq 0$. Then $da + (-(db)) = db + (-(db)) = 0$, which implies that, by a known proposition, $da + d(-b) = 0$, and so by the distributive property, $d(a + (-b)) = 0$. Since $d \neq 0$, and because D is an integral domain, then it must be the case that $a + (-b) = 0$. Finally, $a + (-b) + b = 0 + b$ would imply that $a = b$, as required.

($\Leftarrow$) On the other hand, assume that for all $d \in D$ such that $d \neq 0$, $da = db$ implies $a = b$. Because D is an integral domain, then if $da = 0$, we have that $da = d0$, and so by assumption, $a = 0$. Therefore, d cannot be a zero divisor. $\square$

Definition 1. Let R be a commutative ring with identity. A *polynomial* over a ring R is an expression of the form

$$f(x) = \sum_{i=0}^{n} a_i x^i = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n$$

where for $0 \leq i \leq n$, $a_i \in R$.

Notation. If $f \in R[x]$ is a polynomial, we denote the *degree of f* as $\deg(f)$. If f is a polynomial of degree n, then the coefficient $a_n \in R$ is nonzero and is called the *leading coefficient of f*. A polynomial is called *monic* if the leading coefficient is 1.

Remark 1. Note that in the sense of abstract algebra, we do not think about a polynomial expression as a function. Here, x is an arbitrary symbol, or an object. In this case, we call x the *indeterminate*.

Definition 2. We say that for two polynomials $p(x) = \sum_{i=0}^{n} a_i x^i$ and $q(x) = \sum_{i=0}^{m} b_i x^i$ in $R[x]$ are said to be *equal*, if $n = m$, and for $0 \leq i \leq n$, $a_i = b_i$.

$R[x]$ is a ring with addition over R and polynomial multiplication over R. That is, we will add and multiply coefficients, with respect to the set R we are working with.

Example 1. In $\mathbb{Z}_2[x]$, take $f(x) = 1 + x + x^2$, and $g(x) = x + x^2$. Then

$$\begin{aligned}(f+g)(x) &= (1 + x + x^2) + (x + x^2) \\ &= 1 + 0x + 0x^2 \\ &= 1\end{aligned}$$

[1]Where $\mathbb{F} = \mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$

and

$$\begin{aligned}(fg)(x) &= (1 + x + x^2)(x + x^2) \\ &= x + x^2 + x^3 + x^2 + x^3 + x^4 \\ &= x + 0x^2 + 0x^3 + x^4 \\ &= x + x^4\end{aligned}$$

In general, if R is a commutative ring, then $R[x]$ is also commutative and if R contains the identity, then $R[x]$ is also contains the same identity, i.e. contains the polynomial of degree zero.