Algebra - I
Prof. S. Viswanath & Prof. Amritanshu Prasad
Department of Mathematics
Indian Institute of Technology, Madras

ALGEBRA I

1. Lecture 38: Divisibility and ideals

Let us define divisibility . a divides b if $(b) \subseteq (a)$. An element u is called a unit if there exists v such that $uv = vu = 1$.

The units in the ring of integers $\mathbb{Z}$ are precisely ± 1. The units in the ring of polynomials over a field K are the constant polynomials; the units in the ring of polynomials over a ring R are constant polynomials, whose values must be a unit in the ring R.

Theorem 1.1. *Given elements a, b of an integral domain R, the following are equivalent:*

- $(a) = (b)$
- $b \mid a$ *and* $a \mid b$
- $b = au$, *where u is a unit of the ring R*

Proof. So, we need to show that remains to show that let us say 3 implies 2 . So, we start off by looking at if $b = au$ for some unit u . So, if $b = au$, then obviously, even if u is not a unit, this means that $a \mid b$. Since u is a unit, $bu^{-1} = a$, so b divides a. Clearly 1 implies 2. 2 implies 3 since $b = ra$ and $a = sb$ implies $b(1-rs) = 0$ by distributivity, and in an integral domain, for $b \neq 0$ we must have $rs = 1$ and thus r and s are both units. □

So, what this answers is when the two different elements generate the same principal ideal if they are associates- that is if $a = ub$ for a unit u. So, let us look at some examples .

Example 1.2. *The set of polynomials $f(x) \in \mathbb{Q}[x]$ such that $f(1) = 0$ is an ideal, and is generated by $x - 1$. Clearly this is an ideal, and $(x-1) \subseteq \{f \in \mathbb{Q}[x] | f(1) = 0\}$. By the division algorithm, for each $f \in \{f \in \mathbb{Q}[x] | f(1) = 0\}$ we have*

$$f(x) = (x-1)q(x) + k,$$

for a constant k, which we find to be 0 by evaluating at $x = 0$. Thus $f(x)$ is divisible $x - 1$.

Theorem 1.3 (Factor theorem)**.** *A polynomial $p(x)$ is divisible by $x - a$ iff $p(a) = 0$.*

So, the factor theorem for polynomial says that a polynomial is divisible by x minus a if and only if vanishes ; if and only if it vanishes at a .