

Lecture 14 (Principle Ideal Domains)

Suppose R is a commutative ring. Then for any $a \in R$, aR is an ideal – the principal ideal generated by a .

Definition 14.1 (Principal Ideal Domain) An integral ideal in which every ideal is principal is called a *principal ideal domain*.

For example \mathbb{Z} is a principal ideal domain. We will now show that for any field F and indeterminate x , the polynomial ring $F[x]$ is a principal ideal domain.

Recall Polynomial Long Division.

Lemma 14.2 (Polynomial Long Division) Let F be a field and $f, g \in F[x]$ polynomials with $g \neq 0$. Then there exists unique polynomials q and r in $F[x]$ such that $f = qg + r$ and $\deg r < \deg g$.

Proof (Sketch) Existence.

If $f = 0$ take $q = r = 0$.

Otherwise $\deg f, \deg g \geq 0$. Suppose $\deg f = n$ and $\deg g = m$ and that

$$g = g_0 + g_1x + \cdots + g_mx^m, \quad g_m \neq 0, \quad f = f_0 + f_1x + \cdots + f_nx^n, \quad f_n \neq 0.$$

If $n \geq m$, put $\lambda_0 = f_n g_m^{-1}$. Then $\lambda_0 x^{n-m} g$ and f both have leading term $f_n x^n$. So subtracting times g from f gives a polynomial

$$h = f - \lambda_0 x^{n-m} g$$

with $\deg h < \deg f$. If $n_1 = \deg h \geq \deg g$ we can repeat this process to form a polynomial

$$h_2 = h_1 - \lambda_1 x^{n_1-m} g = f - (\lambda_0 x^{n-m} + \lambda_1 x^{n_1-m}) g$$

with $\deg h_2 < \deg h_1$ etc. After at most $n - m + 1$ this process must end with a polynomial

$$\begin{aligned} h_k &= h_{k-1} - \lambda_k x^{n_{k-1}-m} g \\ &= h_{k-2} - (\lambda_k x^{n_{k-1}-m} + \lambda_{k-1} x^{n_{k-2}-m}) g \\ &= \cdots \\ &= f - (\lambda_k x^{n_{k-1}-m} + \cdots + \lambda_1 x^{n_1-m} + \lambda_0 x^{n_0-m}) g \end{aligned}$$

with $\deg h_k < \deg g$. So setting $r = h_k$, and $q = \sum \lambda_i x^{n_i - m}$ we have, we have $f = qg + r$, $\deg r < \deg g$.

Uniqueness.

Suppose $f = q_1g + r_1 = q_2g + r_2$ with $\deg r_1, \deg r_2 < \deg g$. Then $(q_2 - q_1)g = (r_2 - r_1)$ and $\deg(r_2 - r_1) < \deg g$. But if $q_1 \neq q_2$, $\deg(q_2 - q_1)g = \deg(q_2 - q_1) + \deg g \geq \deg g$. Hence we must have $q_1 = q_2$, and so also $r_1 = r_2$. \square

Comment If you look at the division algorithm for polynomials the only division in the field F of coefficients is division by the coefficient g_m of the leading term of g . So the division algorithm works in any commutative ring R as long as the coefficient of the leading term of g is invertible in R . The uniqueness also follows too because if g has its leading term invertible then $\deg hg = \deg h + \deg g$ holds for all $h \in R[x]$.

Theorem 14.3 If F is a field $F[x]$ is a principal ideal domain.

Proof We know polynomials over a field are an integral domain. It remains to show every ideal is principal. Let I be an ideal of $F[x]$. If $I = 0$, $I = 0F[x]$. Now suppose $I \neq 0$. Let $m(x) \neq 0$ be a polynomial of minimal degree in I . Claim $I = m(x)F[x]$. First $m(x) \in I$ and I an ideal implies all multiples of $m(x)$ lie in I , $m(x)F[x] \subseteq I$. We complete the proof by showing $I \subseteq m(x)F[x]$.

Suppose $f(x) \in I$. Then there are polynomials q and r such that $f = qm + r$ with $\deg r < \deg m$. But $qm \in I$, from above. Because ideals are closed under taking negatives, $-qm \in I$. So because ideals are closed under addition and $f, -qm \in I$, $r = f + (-qm) \in I$. Since m is a non-zero polynomial of minimal positive degree in I , we must have $r = 0$. Hence $f = qm \in m(x)F[x]$. \square

Going back to the division algorithm we recall that in the case $g(x) = x - a$, $a \in F$ the remainder is a constant and we can deduce the following well known result.

Theorem 14.4 (The Remainder Theorem) Suppose F is field, $f \in F[x]$ and $a \in F$. The

(i) The remainder in division of f by $x - a$ is $f(a)$:

$$f(x) = (x - a)q(x) + f(a).$$

(ii) $x - a$ is a factor of $f(x)$ if and only if $f(a) = 0$. \square

Recall that a *non-constant* polynomial is called irreducible if it cannot be written as product of polynomials of strictly lower degree. For example degree 1 polynomials are irreducible.

Note Irreducibility is relative term. The polynomial $x^2 + 1$ is irreducible in $\mathbb{R}[x]$, but $x^2 + 1 = (x + i)(x - i)$ is reducible in $\mathbb{C}[x]$.

Just as every integer is, up to multiplication by ± 1 and the order of factors a product of primes, up to multiplication by constants and the order of factors, every polynomial is uniquely a product of irreducibles.

Division, Associates and Irreducibles

The elementary notions of divisibility for \mathbb{Z} and polynomial domains extended to commutative rings with identity. We are only going to be concerned with divisibility in integral domain but some elementary properties are common to all commutative rings with an identity.

Definition 14.5 (Division) Let R be a commutative ring with a unit element then for $a, b \in R$ we say a divides b and or equivalently a is a factor of b or equivalently and write $a|b$ if b is a multiple of a , viz $b = ac$ for some $c \in R$.

Exercise (Elementary Properties) For all $a, b, c \in R$, a commutative ring with an identity element.

- 1) $a|b$ if and only if $b \in R$ if and only if $Rb \subseteq Ra$.
- 2) $a|b$ and $b|c$ implies $a|c$.
- 3) $a|b$ and $a|c$ implies $a|bx + cy$ for all $x, y \in R$.
- 4) $a|1$ if and only if a is a unit.
- 5) $a|b$ for all $b \in R$ if and only if a is a unit.
- 6) $0|b$ if and only if $b = 0$.
- 7) $a|0$ is always true.

Note only the implication $Rb \subseteq Ra \Rightarrow b \in R$ requires R have an identity.

Definition 14.5 (Associates) Let R be a commutative ring with an identity element. If $a \in R$ an element of the form au is called an associate of a . Write $a \sim b$ if b is an associates of a .

Lemma 14.1 Associativity is an equivalence relation which respects division, i.e. if $a \sim a'$ and $b \sim b'$, $a|b$ if and only if $a'|b'$. The units of R are the associates of 1.

Proof Exercise.

Lemma 14.6 If R is an integral domain then the following are equivalent for $a, b \in R$.

- (i) $a|b$ and $b|a$.
- (ii) $aR = bR$.
- (iii) a and b are associates.

Proof Exercise. (See Homework03). □

Trivial Factorisation Given a pair of units u, v , $uv = 1$ and any a in a commutative ring R then we can factor $a = u(av)$ as product of the unit u , and the associate av of a . This is called a *trivial factorisation*.

Definition 14.7 Let R be an integral domain. A non-zero element of R which is not a unit is called irreducible if its only factors are its associates or units. For example in \mathbb{Z} the irreducible elements are $\pm p$, $p \in \mathbb{N}$ a prime number.