

Lecture 15 (Unique Factorisation Domains)

Recall if R is an integral domain and $\pi \in R \setminus \{0\}$ is called irreducible if it not a unit and its only factors are units or its associates. So if $\pi = ab$, either a is a unit and $b \sim \pi$ or b is a unit and $a \sim \pi$.

Definition 15.1 (Unique Factorisation Domain) An integral domain R is called a *unique factorisation domain* if both the following hold.

- (i) Every non-zero element of $a \in R$ is either a unit or can be expressed as product of irreducibles, i.e. for $a \neq 0$ either $a \in U(R)$ or

$$a = \pi_1 \pi_2 \cdots \pi_n$$

where $\pi_1 \pi_2 \cdots \pi_n \in R$ are irreducible.

- (ii) Factorisation into irreducibles is unique up to associates and the order of factors, i.e. if

$$\pi_1 \pi_2 \cdots \pi_n = \rho_1 \rho_2 \cdots \rho_m$$

with $\pi_1 \pi_2 \cdots \pi_n, \rho_1 \rho_2 \cdots \rho_m \in R$ irreducible then $m = n$ and after a possible renumbering,

$$\pi_1 \sim \rho_1, \quad \pi_2 \sim \rho_2, \quad \dots, \quad \pi_n \sim \rho_n$$

For example \mathbb{Z} is a unique factorisation domain. Every field is a unique factorisation domain, (If F is any field, all non-zero elements are units). If F is any field $F[x]$ is a unique factorisation domain.

In \mathbb{Z} the irreducibles elements are $\pm p$, $p \in \mathbb{N}$ a prime. For \mathbb{Z} the positive irreducible elements, had the property $p|ab$ implies $p|a$ or $p|b$. This stronger notion is taken as the definition of primes in general.

Definition 15.2 An element p of a commutative ring R which is not 0 or a unit is called a *prime* if $p|ab$ implies $p|a$ or $p|b$.

Lemma 15.3 Let R be an integral domain and $p \in R$ a prime. Then p is irreducible.

Proof Suppose $p = ab$. We show one of a, b is a unit and the other an associate of p . Now $p = ab$ implies $p|ab$. So $p|a$ or $p|b$. In the case $p|a$, $a = pc$ for some $c \in R$, which gives $p1 = p = (pc)b = p(bc)$. Because R is an integral domain we conclude $bc = 1$. Hence b and c are units. So $a \sim p$ and b is a unit. In the case $p|b$ we conclude similarly a is a unit and b an associate of p . \square

The converse is not true in general, but it is true for \mathbb{Z} or any $F[x]$, F a field, and more generally in any principal ideal domain R , and the proof is modelled on the case $R = \mathbb{Z}$.

Definition 15.4 (Greatest Common Divisor) Let R be an integral domain and $a, b \in R$ be elements of R which are not both 0. Then $d \in R$ is called a *greatest common divisor* (g.c.d.) of a and b if

GCD(1) $d|a$ and $d|b$;

GCD(2) For all $e \in R$, $e|a$ and $e|b$ then $e|d$.

Lemma Greatest common divisors are non-zero and unique up to associates.

Proof In any commutative ring domain $0|a$, if and only if $a = 0$. So the assumption not both a and b zero implies $d \neq 0$.

If d and d' are greatest common divisors of a and b in some integral domain R , then by GCD(1), $d, d'|a$ and $d, d'|b$. So by GCD(2), $d|d'$ and $d'|d$. Hence d and d' are associates.

Conversely suppose d and d' are associates. Then $d|a$ and $d|b$ if and only if $d'|a$ and $d'|b$ and for any $e \in R$, $e|d$ if and only if $d'|e$. Hence d is a g.c.d. of a and b . \square

Theorem 15.5 Suppose R is a principal ideal domain and a, b pair of elements in R , not both 0,

- (i) Then a and b have a greatest common divisor. Further if d is a g.c.d. of a and b , then $d = ar + bs$ for some $r, s \in R$.
- (ii) If $d \in R$ satisfies $d|a$ and $d|b$ and $d = ar + bs$ for some $r, s \in R$, then d is a greatest common divisor of a and b .

(iii) An element $d \in R$ is a greatest common divisor of a and b if and only if $aR + bR = dR$.

Proof Lets prove (ii) first. Then GCD(1) is assumed and GCD(2) is immediate because $e|a$ and $e|b$ implies $e|ar + bs$ for all r, s in R . (Note this does not use R is a principal ideal domain).

The second half of (i) follows from (iii) since $dR = aR + bR$ implies $d = ar + bs$ for some $r, s \in R$. It remains to show that a and b have a g.c.d. and that (iii) holds.

Set $I = aR + bR = \{ar + bs \mid r, s \in R\}$. Then R a principal ideal domain implies that $I = dR$ for some $d \in R$. We show d is a g.c.d. of a and b . Because R has a unit element, $a \in aR \subseteq I$ and $b \in bR \subseteq I$ and $a, b \in dR$ implies $d|a$ and $d|b$. From the definition of I we have also $d = ar + bs$ for some $r, s \in R$. So by (ii) such a d is a greatest common divisor. We have shown there are $d \in R$ with $aR + bR = dR$ and any such d is greatest common divisor of a and b . Conversely since $dR = d'R$ if and only if d and d' are associates, then by the lemma above we conclude that d is a g.c.d. of a and b if and only if $I = aR + bR = dR$.

□

Proposition 15.6 Let R be a principal ideal domain. Then every irreducible is prime.

Proof Suppose π is an irreducible element of R . Then π is not zero or a unit and its only factors are units and its associates. Hence it has a g.c.d. with any element a of R , and such a g.c.d is either a unit or an associate of π . The latter is the case if and only if $\pi|a$, and the former if and only if $\pi \nmid a$. Now suppose for $a, b \in R$, $\pi|ab$, so $ab = \pi c$ for some $c \in R$. If we show $\pi|a$ or $\pi|b$ then we can conclude π is prime. Suppose $\pi \nmid a$, then a and π have greatest common divisor 1. This implies, by the Theorem above, $1 = ar + \pi s$ for some $r, s \in R$. Hence $b = (ab)r + \pi(bs) = (cr + bs)\pi$ is divisible by π .

□

Corollary For polynomials $F[x]$ a single variable over a field F , irreducible polynomials are prime. □