Lecture 4 Unique Factorization and Eulcidean Domains

January 21, 2021 12:06 PM

In $\mathbb{Z}$ $2 \mid ab \Rightarrow 2 \mid a$ or $2 \mid b$

$2 = a \cdot b \Rightarrow a = \pm 1$ or $b = \pm 1$ (a or b is a unit).

Def. Let R be a comm. ring. and let p be a non-zero element of R which is <u>not a unit</u>.

p is prime if $p \mid ab \Rightarrow p \mid a$ or $p \mid b$.

p is irreducible if $p = a \cdot b \Rightarrow a$ is a unit or b is a unit.

E.g. In $\mathbb{Z}$ $2, -2$ are prime and irreducible.

In $\mathbb{Z}_6$ 2 is prime but not irreducible.

×	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

Is 2 irreducible? $2 = \underline{2 \cdot 4} \Rightarrow 2$ is <u>not</u> irred. (not units)

Is 2 prime? $0 = 2 \cdot 3$ $2 = 2 \cdot 1$ $4 = 2 \cdot 2$

$\Rightarrow 2 \mid 0$ $2 \mid 2$ $2 \mid 4$.

$2 \mid \underline{0} = \underline{3 \cdot 2} = \underline{3 \cdot 4}$

$2 \mid \underline{2} = \underline{2 \cdot 1} = 4 \cdot \underline{2} = 5 \cdot \underline{4}$

$2 \mid \underline{4} = \underline{4 \cdot 1} = \underline{2 \cdot 2} = \underline{4 \cdot 4} = \underline{2 \cdot 5}$

$2 \mid ab \Rightarrow 2 \mid a$ or $2 \mid b$.

Lemma. In an int. dom. D primes are irreducible.

Proof. Let $p = ab$ and p be prime.

Now $p = ab \Rightarrow p \mid ab \Rightarrow p \mid a$ or $p \mid b$.

CASE $p \mid a \Rightarrow p \cdot 1 = (p \cdot \bar{a}) \cdot b \Rightarrow 1 = \bar{a} \cdot b \Rightarrow b$ is a unit.

(p is prime; quotient; CAN CAN)

CASE $p \mid b \Rightarrow p \cdot 1 = a(p \cdot \bar{b}) \Rightarrow p \cdot 1 = p(a\bar{b}) \Rightarrow 1 = a \cdot \bar{b}$

$\Rightarrow a$ is a unit.

(quotient)

Therefore p is irreducible.

Def. An int. dom D is a unique factorization domain (UFD)

Def. An int. dom D is a unique factorization domain (UFD) if $\forall a \in D$ s.t. $a \neq 0$ and $a \notin D^*$,

(i) $a = c_1 \cdot c_2 \cdots \cdot c_r$ for some irreducible $c_i \in D$

(ii) If $a = c_1 c_2 \cdots c_r$ and $a = d_1 d_2 \cdots d_s$ then $r = s$ and $c_i \sim d_j$ for some i and j.

E.g. $\mathbb{Z}$ $12 = 2 \cdot 2 \cdot 3 = 3 \cdot 2 \cdot 2 = (-3) \cdot 2 \cdot (-2)$.

Th. In a UFD irreducibles are prime and gcds exist.

$\mathbb{Q}[\sin, \cos]/(\sin^2 + \cos^2 - 1)$ is an int. dom. but not UFD.

$\sin^2 + \cos^2 = 1 \Rightarrow \sin^2 = 1 - \cos^2$

$\Rightarrow \underline{\sin} \times \underline{\sin} = (1 - \cos)(1 + \cos)$.

$\sin^6 + \cos^6 =$

not units. not associates.

Question: How can we get all different factorizations?

2.4 Euclidean Domains

An int. dom. E is a Euclidean domain if $\exists\ v : E \setminus \{0\} \to \mathbb{N} \cup \{0\}$ [the Euclidean norm] satisfying

(i) $\forall a, b \in E \setminus \{0\}$ $v(a \cdot b) \geq v(a)$

(ii) $\forall a, b \in E$, $b \neq 0$, $\exists q, r \in E$ s.t. $(a \div b)$

$a = bq + r$ and $r = 0$ or $v(r) < v(b)$.

Note: this def makes the Euc. Alg. work. q and r don't have to be unique.

Prop. 1: If u is a unit in E then $v(u) = v(1)$.

Prop. 2: If $a \in E$, $a \neq 0$, a is not a unit $v(a) > v(1)$.

Prop. 1: If u is a unit in E then $v(ua) = v(a)$.

Prop 2: If $a \in E$, $a \neq 0$, a is not a unit $v(a) > v(1)$.

Ex 1. $E = \mathbb{Z}$ $v(x) = |x|$.

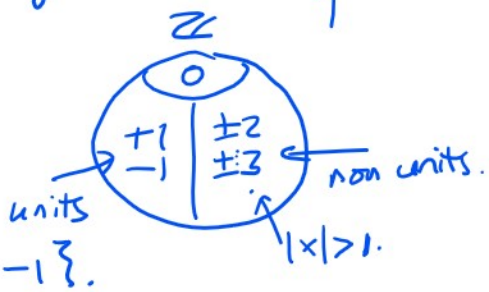
(i) $|ab| = |a| \cdot |b| \geq |a|$.

(ii) $\frac{a \to 11}{b \to 6} = 1 + \frac{5}{6} = 2 + \frac{-1}{6}$ (q, r)

$5 < |6|$ $\quad |-1| < |6|$.

$\gcd(11,6) = \gcd(5,6)$

$\gcd(11,6) = \gcd(-1,6)$



Ex 2. $E = \mathbb{Z}[i] = \{x + iy : x, y \in \mathbb{Z}, i^2 = -1\}$.

$v(a) = |a|^2 = \left(\sqrt{x^2+y^2}\right)^2 = x^2 + y^2$

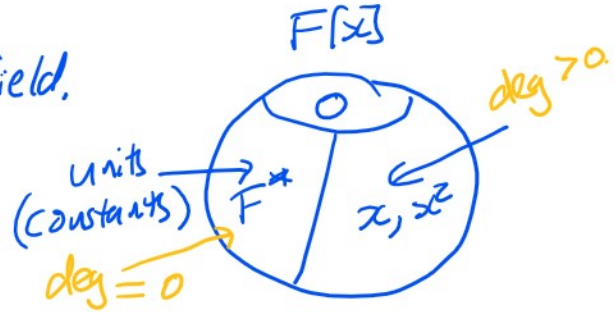
Ex 3. $E = F[x]$ where F is any field.

$v(a) = \deg a$.

(i) $v(ab) = \deg ab$

$= \deg a + \deg b$

$\geq \deg a$



(ii) $b(x) \overline{)\, a(x)}$ with quotient $q(x)$, remainder $r(x)$

$r(x) = 0$ or $\deg r(x) < \deg b(x)$.

Ex 4. $E = F$ a field.

(i) $v(a) = 1$

(ii) $q = a/b = a \cdot b^{-1}$, $r = 0$.

Theorem. All fields are Euclidean domains.

Theorem All Euclidean domains are UFDs.

Proof of Prop 1. $v(u) = v(1)$.

$v(u) = v(1 \cdot u) \geq v(1)$

$v(1) = v(u \cdot u^{-1}) \overset{(i)}{\geq} v(u)$

$v(1) \geq v(u)$ and $v(u) \geq v(1) \Rightarrow v(u) = v(1)$.

Prop 2. $v(a) > v(1)$ (a is not a unit.) $\Leftarrow$ $1 \div a$.

Let $1 = a \cdot q + r$ with $r = 0$ or $v(r) < v(a)$.

CASE $r = 0$: $\Rightarrow 1 = a \cdot q \Rightarrow a$ is a unit. ☒

CASE $r \neq 0$ $v(r) < v(a)$

$v(r) = v(1 \cdot r) \geq v(1)$. by (i).

$v(a) > v(r) \geq v(1) \Rightarrow v(a) > v(1)$.