Groups & Rings: Lecture #20

Unique factorization (§18.2)

- Prime & irreducible
- UFD
- PID $\Rightarrow$ UFD
- ED $\Rightarrow$ PID
- Quadratic integers $\mathbb{Z}[\sqrt{D}]$, $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$
- Noetherian rings

Prime and irreducible elements

Let D be an integral domain.

Recall: $x \in D$ **irreducible** if non-zero, non-unit and $\nexists\, x = yz$ (y, z non-units).

Def: $x \in D$ **prime** if

(i) non-zero

(ii) non-unit $\iff (x) \neq D$

(iii) $x \mid ab \implies x \mid a$ or $x \mid b$

$\iff (x)$ prime ideal

$ab \in (x)$ $\quad a \in (x)$ $\quad b \in (x)$

Ex: $n \in \mathbb{Z}$ irreducible $\iff n = \pm p \iff n$ is prime.

Ex 18.8: $D = \mathbb{Q}[x^2, xy, y^2] \subset \mathbb{Q}[x, y]$ smallest subring containing x^2, xy, y^2

$D \xleftarrow{\sim} \mathbb{Q}[u, v, w]/(uw - v^2)$

1st iso for ϕ

$\mathbb{Q}[u, v, w] \xrightarrow{\phi} \mathbb{Q}[x, y]$ evaluation hom.

$u \longmapsto x^2$

$v \longmapsto xy$

$w \longmapsto y^2$

$\operatorname{im} \phi = D$

$\ker \phi = (uw - v^2)$

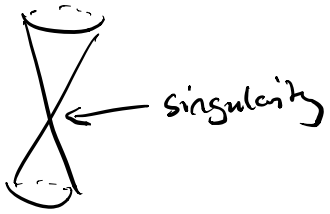
$xy = \bar{v}$ is irreducible (b/c deg = 2 smallest possible > 0 in D)

but not prime $\quad xy \mid x^2 \cdot y^2$ $\quad \bar{v} \mid \bar{u} \cdot \bar{w}$

$xy \nmid x^2, \quad xy \nmid y^2$ $\quad \bar{v} \nmid \bar{u}, \ \bar{v} \nmid \bar{w}$

Geometrical explanation of example:

The surface $\{uw - v^2 = 0\} \subset \mathbb{R}^3$ has a singularity at the origin



Lemma (Exc 18.5) prime $\Rightarrow$ irreducible.

pf: Suppose $x \in D$ is prime. Then x non-zero, non-unit.

Suppose $x = yz$.

Then $x \mid yz \Longrightarrow$ either $x \mid y$ or $x \mid z$.

Suppose $x \mid y$. Then $y = xa$.

$\Rightarrow x = yz = xaz \Longrightarrow 1 = az \Rightarrow a, z$ units

(D domain)

Similarly $x \mid z \Rightarrow y$ unit.

$\Rightarrow x$ is irreducible. $\square$

Unique Factorization Domains (UFD)

Ex: In $\mathbb{Z}$ can factor integers into primes (unique up to order and sign):

$n = \pm p_1 \cdot p_2 \cdot p_3 \cdot \cdots \cdot p_m$, p_i primes

Def: D is **UFD** if:

(i) EXISTENCE $\forall x \in D$ non-zero, non-unit

$\exists\, x = y_1 y_2 \cdots y_m$ y_i irreducible

(ii) UNIQUENESS For two such factorizations

$x = y_1 y_2 \cdots y_m = z_1 z_2 \cdots z_n$ we have:

- $m = n$
- $y_i = \text{unit} \cdot z_{\sigma(i)}$ $\forall i$, for some permutation $\sigma \in S_n$.

Ex: $\mathbb{Z}$ is a UFD. $(\mathbb{Z}^\times = \{\pm 1\})$

Rmk: $y = \text{unit} \cdot z \iff (y) = (z)$

Def: y, z are **associate** if $(y) = (z)$.

Ex: $\mathbb{Q}[x^2, xy, y^2]$ is not a UFD: $x^2y^2 = x^2 \cdot y^2 = xy \cdot xy$

(different factorizations)

Ex: $\mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} : a, b \in \mathbb{Z}\} \subset \mathbb{C}$ is not a UFD

$4 = 2 \cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3}) = a \cdot b \cdot c \cdot d$?

$= 1^2 - (-3) = 4$

Are 2, $1+\sqrt{-3}$, $1-\sqrt{-3}$ irreducible? If not

Answer: yes, irreducible (but not prime): use norm (later)

Ex: $\mathbb{Z}[\sqrt{-5}]$ not UFD: $9 = 3 \cdot 3 = (2+\sqrt{-5})(2-\sqrt{-5}) = 4+5$

Again 3, $2+\sqrt{-5}$, $2-\sqrt{-5}$ are irreducible (but not prime)

Rmk: (i) Existence in def of UFD holds "almost always" Enough that D is a noetherian ring. (later)

Theorem (~ Cor 18.13) If D is a UFD, then irreducible $\Rightarrow$ prime.

pf: Suppose $x \in D$ irreducible. Then x is non-zero, non-unit.
Suppose $x \mid ab$. Then $ab = xy$.
UFD $\Rightarrow \exists a = a_1 a_2 \cdots a_m$, $b = b_1 b_2 \cdots b_n$ a_i, b_j irr.
((i) existence part) $y = y_1 y_2 \cdots y_s$

$$a_1 a_2 \cdots a_m b_1 b_2 \cdots b_n = x y_1 y_2 \cdots y_s$$ factorization into irreducibles

UFD $\Rightarrow$ ((ii) uniqueness part) $x = \text{unit} \cdot a_i$ or $x = \text{unit} \cdot b_j$ $\Rightarrow$ $x \mid a$ or $x \mid b$ □

Theorem (pf of Thm 18.15) If irreducible $\Rightarrow$ prime, then uniqueness of factorization (UFD (ii)) holds.

pf: Suppose $x = a_1 a_2 \cdots a_m = b_1 b_2 \cdots b_n$ a_i, b_j irreducible. $\Downarrow$ prime
WLOG $m \le n$.
Since $a_1 \mid b_1 b_2 \cdots b_n \Rightarrow a_1 \mid b_j$ for some j
WLOG: $j = 1$. So $b_1 = a_1 u_1$ where u_1 unit since b_1 irr.
$\Rightarrow a_2 \cdots a_m = u_1 b_2 \cdots b_n \xrightarrow[\text{repeat arg}]{\Rightarrow} b_2 = a_2 u_2 \Rightarrow \cdots \Rightarrow b_n = a_n u_n$
$\Rightarrow 1 = u_1 u_2 \cdots u_m \underbrace{b_{m+1} \cdots b_n}_{\Rightarrow \text{unit}} \Rightarrow m = n$ □

Corollary: If D noetherian then (irreducible $\Rightarrow$ prime) $\Leftrightarrow$ UFD

PID ⇒ UFD

PID = principal ideal domain = every ideal is principal

Ex: $\mathbb{Z}$, $F[x]$ PIDs. (proof div. alg.)

Non-ex: $F[x,y]$ not PID. $(x,y) = \{xp(x,y) + yq(x,y)\}$
not principal $= \{p(x,y) : p(0,0) = 0\}$

Theorem (18.12) D PID, $x \in D$. Then
x irreducible $\iff$ (x) maximal (and non-trivial)

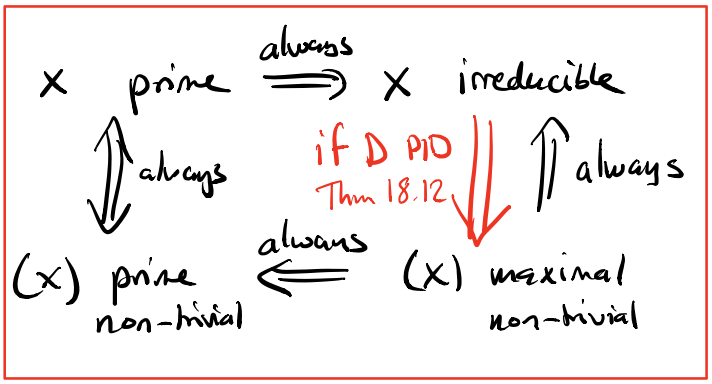
pf: (x non-zero $\iff$ (x) non-trivial)
x non-unit $\iff$ (x) proper ($\neq D$)

($\Leftarrow$) always true
Suppose (x) maximal. Suppose $x = yz$, y, z are not units
Then $(x) \subsetneq (y) \subsetneq D$. Contradicts (x) maximal.
(z not unit; y not unit)

($\Rightarrow$) Suppose x irreducible. Suppose $(x) \subsetneq I \subsetneq D$
$\Rightarrow y \mid x$, $x = yz$
contradicts x irreducible.
(z not unit; $I = (y)$; D PID; y not unit) □

Cor: If D PID, then irreducible $\Rightarrow$ prime.
($\Rightarrow$ uniqueness of fact.)

proof: See diagram →



Fact: PID ⇒ Noetherian.
(later) ($\Rightarrow$ existence of fact.)

Conclude: PID ⇒ UFD.

Euclidean domains

Def: D is a **Euclidean domain** if $\exists$ **Euclidean function** υ

$\upsilon : D \setminus \{0\} \longrightarrow \mathbb{N}$ s.th.

(EF1) $a, b \in D$, $b \neq 0$ $\exists\, a = qb + r$ $\upsilon(r) < \upsilon(b)$ or $r = 0$

(EF2) $\upsilon(a) \leq \upsilon(ab)$ $\forall a, b \neq 0$.

(not need in all sources, not on lecture #19, in book)

Thm: Euclidean domain (ED) $\Rightarrow$ PID. (EF1 is enough)

pf: Use div. algo just as for $\mathbb{Z}$ and $F[x]$.

Ex: The **Gaussian integers** $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ is a ED.

The **norm** is a multiplicative Euclidean function. $N : \mathbb{Z}[i] \to \mathbb{N}$

$$N(a+bi) = |a+bi|^2 = (a+bi)(a-bi) = a^2 + b^2$$

$$N(z) = z\bar{z}$$

$$N(zw) = N(z)N(w) \quad (N \text{ is multiplicative})$$

If z is a unit: $\exists z^{-1} : zz^{-1} = 1 \Rightarrow N(z)N(z^{-1}) = N(zz^{-1}) = 1$

$\Rightarrow N(z)$ is a unit $\Rightarrow N(z) = 1$.

Potential units: $a+bi$, $a^2 + b^2 = 1 \Rightarrow (a,b) = (\pm 1, 0)$ $(a,b) = (0, \pm 1)$

$1, -1, i, -i$.

Rmk: $N(z) = z\bar{z} = 1 \Rightarrow z^{-1} = \bar{z}$

Fact: N is a Euclidean function (see book 18.20).

Quadratic Integers

(see supplementary material on course web page)

Fix $D \in \mathbb{Z}$ squarefree (no repeated prime factors)

QUADRATIC NUMBERS (FIELD)

- $\mathbb{Q}(\sqrt{D}) := \{a + b\sqrt{D} : a, b \in \mathbb{Q}\} \subset \mathbb{C}$

  is 1st iso thm for ϕ

  $\mathbb{Q}[x]/(x^2 - D)$

$$\phi : \mathbb{Q}[x] \longrightarrow \mathbb{C}, \quad x \longmapsto \sqrt{D}$$

QUADRATIC INTEGERS (DOMAINS)

- $\mathbb{Z}[\sqrt{D}] = \{a + b\sqrt{D} : a, b \in \mathbb{Z}\} \cong \mathbb{Z}[x]/(x^2 - D)$

  $\cap$ ← sometimes equality ($D \not\equiv 1 \bmod 4$)

- $\mathcal{O}_{\mathbb{Q}(\sqrt{D})} = \{z = a + b\sqrt{D} : a, b \in \mathbb{Q},\ N(z), \mathrm{tr}(z) \in \mathbb{Z}\}$ (see below)

  $\cap$

  $\mathbb{Q}(\sqrt{D})$

CONJUGATION

$$\sigma : \mathbb{Q}(\sqrt{D}) \longrightarrow \mathbb{Q}(\sqrt{D})$$

$$a + b\sqrt{D} \longmapsto \overline{(a + b\sqrt{D})} := a - b\sqrt{D}$$

WARNING: σ coincides with usual complex conjugation $\Leftrightarrow D < 0$

NORM

$N : \mathbb{Q}(\sqrt{D}) \longrightarrow \mathbb{Q}$ (multiplicative function)

$z = a + b\sqrt{D} \longmapsto z\bar{z}$ $\quad (a + b\sqrt{D})(a - b\sqrt{D}) = a^2 - b^2 D$

TRACE

$\mathrm{tr} : \mathbb{Q}(\sqrt{D}) \longrightarrow \mathbb{Q}$ (additive function, i.e. group homo for $+$)

$$z \longmapsto z + \bar{z}$$

$$a + b\sqrt{D} \longmapsto 2a$$

Prop: (see supp material)

$$\mathcal{O}_{\mathbb{Q}(\sqrt{D})} = \mathbb{Z}[\omega] = \{a+b\omega : a,b \in \mathbb{Z}\}$$

where $\omega \in \mathbb{Q}(\sqrt{D})$ is:

$$\omega = \begin{cases} \sqrt{D} & \text{if } D \not\equiv 1 \pmod 4 \\ \frac{1}{2}(1+\sqrt{D}) & \text{if } D \equiv 1 \pmod 4 \end{cases}$$

Ex: $D=-3$, $\quad 4 = 2\cdot 2 = (1+\sqrt{-3})(1-\sqrt{-3})$

$$N(4) = N(2)\cdot N(2) = N(1+\sqrt{-3})N(1-\sqrt{-3})$$

$$N: \mathbb{Z}[\sqrt{D}] \longrightarrow \mathbb{Z}$$

$$a+b\sqrt{-3} \longmapsto (a+b\sqrt{-3})(a-b\sqrt{-3}) = a^2+3b^2$$

$N(2) = 2^2 = 4$

$N(1\pm\sqrt{-3}) = 1+3 = 4$

$N(a), N(b) \neq \pm 1 \iff (*)$

If 2 was not irreducible $\Rightarrow 2 = a\cdot b$, a,b not units

$$\Rightarrow N(2) = N(a)N(b)$$
$$\quad\;\; \| \qquad \| \quad \| $$
$$\quad\;\; 4 \qquad 2 \quad 2$$

Lemma $(*)$: $a \in \mathbb{Z}[\sqrt{D}]$ or $a \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$. Then invertible $\iff N(a) = \pm 1$.

proof: $a\alpha^{-1} = 1 \Rightarrow N(a)N(\alpha^{-1}) = 1 \Rightarrow N(a) = \pm 1$

$N(a) = \pm 1 \Rightarrow a\bar{a} = \pm 1 \Rightarrow a^{-1} = \pm\bar{a}$ □

$\exists\, p,q \in \mathbb{Z} : N(p+q\sqrt{-3}) = 2$?

$$\| $$

$$p^2+3q^2$$

$\nexists\, p+q\sqrt{-3}$ with norm 2 ←

p	q	$N(p+q\sqrt{-3})$
0	1	3
1	0	1
1	1	4
2	0	4
0	2	12

$\Rightarrow$ 2 & $1\pm\sqrt{-3}$ are irreducible.

Noetherian Rings (not on lecture)

Def: A ring R is noetherian if every ascending chain of ideals

$$I_1 \subseteq I_2 \subseteq \cdots$$

stabilizes, that is, $\exists N$: $I_N = I_{N+1} = \cdots$

Lemma 18.14: A PID D is noetherian.

pf: Let $I_1 \subseteq I_2 \subseteq \cdots$ be an ascending chain of ideals.

Let $I = \bigcup_{n \geq 1} I_n$. This is an ideal (easy exercise).

Thus $I = (f)$ for some $f \in D$ because D PID.

Then $f \in I_n$ for some n.

$\Rightarrow (f) \subset I_n \subset I_{n+1} \subset \cdots \subset I = (f)$.

$\Rightarrow I_n = I_{n+1} = \cdots = I$ □

(**Fact:** $F[x_1, x_2, \ldots, x_n]$ also noetherian. In fact R noeth $\Rightarrow R[x]$ noeth.)

Lemma (Thm 18.15 part 1) If D noetherian domain, then factorizations into irreducibles exist.

pf: Suppose $x \in D$, non-unit, non-zero, does not have a factorization into irreducibles.

Let $x_1 := x$. Since x_1 not irreducible, $x_1 = yz$, y, z not units.

Either y or z (or both) does not have a factorization.

Say y doesn't and let $x_2 := y$.

Continuing, we get $(x_1) \subsetneq (x_2) \subsetneq (x_3) \subsetneq \cdots$ contradicting D noetherian. □