Introduction to Rings and Modules

Lecture 7, Monday May 8 2023
Ari Feiglin

Definition 7.0.1:

An integral domain R is called a **euclidean domain** if there exists a function

$$N\colon R \longrightarrow \mathbb{N}_{\geq 0}$$

such that $N(0_R) = 0$ and for every $a, b \in R$ where $b \neq 0$, there exist $q, r \in R$ such that $a = bq + r$ and $r = 0$ and $N(r) < N(b)$.

Example 7.0.2:

(1) $R = \mathbb{Z}$ is a euclidean domain with norm $N(a) = |a|$ (by the euclidean algorithm).

(2) If F is a field and $N(a) = 0$ then for every $a \in F$ and $0 \neq b \in F$ we have $a = b(b^{-1}a) + 0$.

(3) If $R = F[x]$ where F is a field, let $N(p)$ be the degree of the polynomial p (the maximum index of x^k whose coefficient is non-zero). But we need to show that R is an integral domain, but we showed that if R is an integral domain, so is $R[x]$ (since the leading coefficient of the product of two polynomials is $a_n b_m$, and if this is zero, then $a_n b_m = 0$ so $a_n = 0$ or $b_m = 0$ in contradiction).

(4) $R = \mathbb{Z}[i] = \{a + bi \mid a + b \in \mathbb{Z}\}$, this is a subring of $\mathbb{C}$ since it is obviously an additive subgroup, and

$$(a + bi)(c + di) = ac - bd + i(ad + bc) \in \mathbb{Z}[i]$$

and $1 = 1 + 0i \in \mathbb{Z}[i]$, so $\mathbb{Z}[i] \leq \mathbb{C}$ as required. $\mathbb{Z}[i]$ is an integral domain since $\mathbb{C}$ is a field (and therefore an integral domain).
The norm here is $N(z) = |z|^2$, which is natural as it is equal to $a^2 + b^2$. Obviously $N(0) = 0$. Notice that the norm is multiplicative: $N(zw) = |zw|^2 = |z|^2|w|^2 = N(z)N(w)$.
Let $z, w \in \mathbb{Z}[i]$ where $w \neq 0$, we can take $\alpha = \frac{z}{w} \in \mathbb{C}$. Thus there exists $n, m \in \mathbb{Z}$ such that $|\Re\alpha - n| \leq \frac{1}{2}$ and $|\Im\alpha - m| \leq \frac{1}{2}$. Let $q = n + mi$ and $r = z - wq$, we claim $r = 0$ or $N(r) < N(w)$. We know that

$$\gamma - q = \Re\gamma - n + i\big(\Im\gamma - m\big) \implies |\gamma - q|^2 = |\Re\gamma - n|^2 + |\Im\gamma - m|^2 \leq \frac{1}{2}$$

And since

$$N(r) = N(z - wq) = |z - wq|^2 = |w|^2 \cdot |\gamma - q|^2 \leq \frac{1}{2}|w|^2 = \frac{1}{2}|w|^2 = \frac{1}{2}N(w)$$

So if $r \neq 0$ then $N(r) \neq 0$ so $N(w) \neq 0$ and therefore $N(r) \leq \frac{1}{2}N(w) < N(w)$ as required.

Proposition 7.0.3:

Every euclidean domain is a prime ideal domain (PID).

Since we showed that $\dim \mathbb{Z}[x] \geq 2$ as (x) and $(2, x)$ are prime ideals in $\mathbb{Z}[x]$, $\mathbb{Z}[x]$ is not a principal ideal domain and therefore not euclidean.

Proof:

Let $I \triangleleft R$ be an ideal of R, if I is trivial then I is principal. Otherwise $I \neq (0_R)$, let

$$n = \min\{N(a) \mid a \in I, a \neq 0\}$$

there exists a $0 \neq d \in I$ such that $N(d) = n$, and we claim $(d) = I$. $(d) \subseteq I$ since $d \in I$. And if $a \in I$ there exists

$q, r \in R$ such that $a = dq + r$ and $r = 0$ or $N(r) < N(d)$ since $d \neq 0$. Then $dq \in I$ and $a \in I$ so $a - dq = r \in I$, and so $N(d) \geq N(r)$ since $N(d)$ is a minimum and therefore $r = 0$. Therefore $a = dq$ so $a \in (d)$ as required. ■

Definition 7.0.4:

A ring R is left/right **Noetherian** if every ascending chain of left/right ideals stabilizes, that is for every ascending chain of left/right ideals

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

there exists an N such that $I_N = I_{N+1} = \cdots$. If a ring is both left and right Noetherian, it is also just called Noetherian.

Example 7.0.5:

(1) Finite rings are Noetherian.

(2) $\mathbb{Z}$ is a PID and $(n) \subseteq (m)$ if and only if $m \mid n$, and so $\mathbb{Z}$ is also Noetherian.

Proposition 7.0.6:

Every PID is Noetherian.

Proof:

Suppose $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ be an ascending chain of real ideals (if $I_i = I$ it is trivial that this stabilizies). Let

$$I = \bigcup_{i=1}^{\infty} I_i$$

and we have already shown that this is an ideal in our proof of the existence of maximal ideals. Since R is a principal integral domain, $I = (a)$ for some $a \in R$, thus $a \in \bigcup_{i=1}^{\infty} I_i$ so there exists an i such that $a \in I_i$. So $(a) \subseteq I_i \subseteq I = (a)$ and so $I_i = (a)$ and for every $j \geq i$, $(a) = I_i \subseteq I_j \subseteq I = (a)$ so $I_j = (a)$ and therefore the chain stabilizes to I, as required. ■

Proposition 7.0.7:

A ring R is left/right Noetherian if and only if every left/right ideal is finitely generated.

Proof:

Let us show this for the left case. Let us denote $Rx_1 + \cdots + Rx_n$ by $R(x_1, \ldots, x_n)$. If every left ideal is finitely generated, let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots$ be an ascending chain of ideals, then

$$I = \bigcup_{i=1}^{\infty} I_i$$

is an ideal, and so $I = R(x_1, \ldots, x_n)$ and therefore for every $1 \leq k \leq n$, $x_k \in I_{i_k}$ for some i_k. Let $N = \max\{i_k \mid 1 \leq k \leq n\}$, then every x_k is in I_N and so $(x_1, \ldots, x_n) \subseteq I_N \subseteq I = R(x_1, \ldots, x_n)$ so $I_N = R(x_1, \ldots, x_n)$. And for every $M \geq N$, $R(x_1, \ldots, x_n) = I_N \subseteq I_M \subseteq I = R(x_1, \ldots, x_n)$ so $I_M = R(x_1, \ldots, x_n) = I$ for every $M \geq N$, so R is left Noetherian.
Now suppose R is left Noetherian. Suppose that I is a left ideal which is not finitely generated. We construct a non-stabilizing chain recursively like so: let $a_1 \in I$ and define $I_1 = R(a_1)$. Then $I_1 \subset I$ strictly as I is not finitely generated, so there exists $a_2 \in I \setminus I_1$, and let $I_2 = R(a_1, a_2)$. And inductively there exists an $a_{n+1} \in I \setminus I_n$, and let $I_{n+1} = R(a_1, \ldots, a_n, a_{n+1})$. So $I_n \subset I_{n+1}$ strictly, so this chain cannot stabilize in contradiction. ■

Definition 7.0.8:

Let R be a ring. If every descending chain of left/right ideals stabilizes, R is called left/right **Artinian**. If R is both left and right Artinian, it is also just caleld Artinian.

Example 7.0.9:

$\mathbb{Z}$ is not Artinian since

$$2\mathbb{Z} \supset 4\mathbb{Z} \supset 8\mathbb{Z} \supset 16\mathbb{Z} \supset \cdots$$

is a non-stabilizing descending chain of ideals.