2. Euclidean domains and polynomial rings (Chapter II.3, II.4)

R - integral domain

Definition 2.1. R is called a *euclidean domain* if $\exists$ function $\varphi: R \longrightarrow \mathbb{Z}$ such that:
(i) if $a, b \in R^*$ and $b \mid a$, then $\varphi(b) \leq \varphi(a)$, and
(ii) if $a \in R$ and $b \in R^*$, then $\exists\, q, r \in R$ with $a = bq + r$ and $\varphi(r) < \varphi(b)$.

Theorem 2.2. Let (R, φ) be a euclidean domain. Then R is a PID.

Proof. Let $I \subseteq R$ be a nonzero ideal. The set

$$\varphi(I^*) = \{\varphi(a) \mid a \in I \setminus \{0\}\}$$

is not empty, since $I \neq (0)$. Moreover, $1 \mid a \Rightarrow \varphi(1) \leq \varphi(a)$ $\forall a \in R$. Hence $\varphi(1)$ is a lower bound for $\varphi(I^*)$. By the well-ordering principle, there exists $n_0 \in \varphi(I^*)$ such that

$$n_0 \leq \varphi(a) \quad \forall\, a \in I \setminus \{0\}.$$

Let $b \in I \setminus \{0\}$ be such that $\varphi(b) = n_0$. Then $(b) \subseteq I$ and it is enough to show $I \subseteq (b)$.

Let $a \in I$. Since (R, φ) is a euclidean domain, there exist $q, r \in R$ with $a = bq + r$ and $\varphi(r) < \varphi(b)$. Since

$$r = a - bq \in I$$

and $\varphi(r) < \varphi(b) = n_0$, we have $r = 0$. Hence $a = bq \in (b)$ and so $I \subseteq (b)$. $\square$

In particular, using Theorem 1.6 we have

$$R \text{ euclidean domain} \Rightarrow R \text{ PID} \Rightarrow R \text{ UFD}.$$

Example 2.3 (1) $\mathbb{Z}$ with $\varphi(n)=|n|$ is a euclidean domain.
(2) $F[x]$ where F is a field with

$$\varphi(f(x))=\begin{cases}\deg(f), & \text{if } f(x)\neq 0,\\ -1, & \text{if } f(x)=0,\end{cases}$$

is a euclidean domain.
(3) $\mathbb{Z}[i]=\{a+bi \mid a,b\in\mathbb{Z}\}$, known as the ring of Gaussian integers with $\varphi(a+bi)=a^2+b^2$ is a euclidean domain.
(4) There exist PIDs that are not euclidean domains, see Remark 11.3.3.

Now we turn our attention to polynomial rings, which are very important in this course.

Theorem 2.4. (Generalized division). Let

$$f(x)=f_0+f_1x+\cdots+f_mx^m\in R[x]$$
$$g(x)=g_0+g_1x+\cdots+g_nx^n\in R[x]^*$$

Set $k:=\max\{m-n+1,0\}$. Then $\exists!\, q(x),r(x)\in R[x]$ such that

$$g_n^k f(x)=q(x)g(x)+r(x),$$

where $\deg(r)<\deg(g)$ $(\deg(0)=-\infty)$.

Proof. Case $m<n$: $q(x)=0$, $r(x)=f(x)$.
Case $m\geq n$: we use induction on m. For the base case $m=0$, we have $q(x)=f_0$, $r(x)=0$. For the induction step, assume the claim true for polynomials of degree less than m. Then

$$d:=\deg(g_nf(x)-f_mx^{m-n}g(x))\leq m-1$$

induction hypothesis

$\exists\, q_1(x),r_1(x)\in R[x]$ such that

$$g_u^{k'}\left(g_u f(x) - F_m x^{u-m} g(x)\right) = q_1(x) g(x) + r_1(x), \quad \deg(r) < \deg(g),$$

where $k' = \max\{d-u+1, 0\}$. By rearranging, we obtain

$$g_u^{k'+1} F(x) = \left(q_1(x) + f_m g_u^{k'} x^{m-u}\right) g(x) + r_1(x), \quad \deg(r) < \deg(g). \quad (1)$$

We claim that $k := \max\{m-u+1, 0\} \geq k'+1$. Indeed, using the general formula

$$\max\{a,b\} = \frac{1}{2}(a+b+|a-b|) \quad \text{for } a, b \in \mathbb{R},$$

we have

$$\begin{aligned} k-(k'+1) &= \max\{m-u+1, 0\} - (\max\{d-u+1, 0\} + 1) \\ &= \frac{1}{2}(m-u+1+|m-u+1|) - \frac{1}{2}(d-u+1+|d-u+1|) - 1 \\ (m \geq u) \quad &= \frac{1}{2}(m-u+1+m-u+1-d+u-1+|d-u+1|-2) \\ &= \frac{1}{2}(2m-u-1-d+|d-u+1|) \\ &= \begin{cases} \frac{1}{2}(2m-u-1-d+d-u+1), & \text{if } d-u+1 \geq 0 \\ \frac{1}{2}(2m-u-1-d-(d-u+1)), & \text{if } d-u+1 < 0 \end{cases} \\ &= \begin{cases} \frac{1}{2}(2m-2u), & \text{if } d-u+1 \geq 0 \\ \frac{1}{2}(2m-2d-2), & \text{if } d-u+1 < 0 \end{cases} \\ &= \begin{cases} m-u \geq 0 \quad (\text{since } m \geq u) \\ m-(d+1) \geq 0 \quad (\text{since } d \leq m-1). \end{cases} \end{aligned}$$

Since $k-(k'+1) \geq 0$, we have that $g_u^{k-(k'+1)} \in R$. Multiplying (1) by $g_u^{k-(k'+1)}$, we obtain

$$g_u^k F(x) = \underbrace{g_u^{k-(k'+1)}\left(q_1(x) + F_m g_u^{k'} x^{m-u}\right)}_{:= q(x)} g(x) + \underbrace{g_u^{k-(k'+1)} r_1(x)}_{:= r(x)}$$

And setting we have $g_u^k F(x) = q(x) g(x) + r(x)$, $\deg(r) < \deg(q)$, as required.

For uniqueness, note that if

$$g_u^k f(x) = q_1(x) g(x) + r_1(x) = q_2(x) g(x) + r_2(x), \quad \begin{matrix} \deg(r_1) < \deg(g) \\ \deg(r_2) < \deg(g) \end{matrix}$$

then

$$\left(q_1(x) - q_2(x)\right) g(x) = r_2(x) - r_1(x).$$

Assuming $q_1(x)-q_2(x)\neq 0$ and taking degrees, we obtain

$$\deg(g(x)) > \deg(r_2(x)-r_1(x)) = \deg(q_1(x)-q_2(x)) + \deg(g(x)) \geq \deg(g(x)),$$

which is a contradiction. Hence $q_1(x)=q_2(x)$ and so $r_1(x)=r_2(x)$. □

Remark 2.5 Although generalized division holds in $R[x]$ over any ring, $R[x]$ is not a euclidean domain in general. It is, however, when R is a field.

For the rest of this lecture we assume that R is a UFD. We show that $R[x]$ is a UFD. This is a generalization of $F[x]$ being a UFD when F is a field.

Definition 2.6 Let $f(x)=a_0+a_1x+\cdots+a_nx^n \in R[x]$.

(1) $f(x)$ is called monic if $a_n=1$

(2) The content of $f(x)$, denoted $c(f)$, is

$$c(f) := \gcd(a_0, a_1, \ldots, a_n).$$

(3) We say that f is primitive if $c(f)=1$

Lemma 2.7 (Gauss' Lemma) If $f(x), g(x) \in R[x]$, then $c(fg)=c(f)c(g)$.

Proof. Set $c := c(f)$, $d := c(g)$. Then

$$f(x) = cf_1(x), \quad f_1(x) \text{ primitive}$$

$$g(x) = dg_1(x), \quad g_1(x) \text{ primitive}$$

$$f(x)g(x) = (cd)f_1(x)g_1(x).$$

Hence it is enough to show that f_1g_1 is primitive. Assume instead that exists irreducible $p \in R$ which divides all coefficients of f_1g_1. Let

$$f_1(x) = a_0+a_1x+\cdots+a_nx^n,$$

$$g_1(x) = b_0+b_1x+\cdots+b_mx^m.$$

Let a_s, b_t be minimal such that $p \nmid a_s$, $p \nmid b_t$. Then

the coefficient of x^{s+t} in $f_1 g_1$ is

$$\cdots + a_{s-2}b_{t+2} + a_{s-1}b_{t+1} + a_s b_t + a_{s+1}b_{t-1} + a_{s+2}b_{t-2} + \cdots$$

and is divisible by p, by assumption. Since

$$p \mid a_0, p \mid a_1, \ldots, p \mid a_{s-1}, p \mid b_0, p \mid b_1, \ldots, p \mid b_{t-1},$$

it follows that $p \mid a_s b_t$. But this contradicts R being a UFD. □

Theorem 2.8 Assume that R is a UFD. Then $R[x]$ is a UFD.

Proof (sketch). We give a sketch of the proof in the case $R = \mathbb{Z}$.

First step: show that a primitive polynomial in $\mathbb{Z}[x]$ is irreducible if and only if it is irreducible in $\mathbb{Q}[x]$.

Second step: let $f(x) \in \mathbb{Z}[x]$ and $c := c(f)$. Write $f(x) = c f_1(x)$, where $f_1(x)$ is primitive. Find a factorization

$$f_1(x) = \lambda p_1(x) \cdots p_n(x) \quad \text{in } \mathbb{Q}$$

where $\lambda \in \mathbb{Q}$ and $p_1, \ldots, p_n \in \mathbb{Z}[x]$ are primitive and irreducible in $\mathbb{Q}[x]$ (this can be done because $\mathbb{Q}$ is a field).

Third step: by Gauss' Lemma we have that $p_1 \cdots p_n$ is primitive. Since f_1 is also primitive, conclude that $\lambda = 1$.

Fourth step: from all the above steps we obtain a factorization

$$f(x) = c \cdot p_1(x) \cdots p_n(x)$$

where all terms are irreducible. Uniqueness follows by uniqueness of factorization in $\mathbb{Q}[x]$. □