

21.

Euclidean domainsFix a commutative ring R .Def: A norm on R is a function $R \rightarrow \mathbb{N}$ with $0 \mapsto 0$ A norm N is positive if $N(a) > 0 \quad \forall a \neq 0$.A domain R is Euclidean if \exists norm $N: R \rightarrow \mathbb{N}$ such that $a, b \in R$ with $b \neq 0 \Rightarrow \exists q, r \in R$ satisfying

$$a = qb + r \quad \text{with } r = 0 \text{ or } N(r) < N(b)$$

quotient remainder

E.g. • $R = \text{field } \mathbb{k}$, $N = \text{anything: } a = qb$ for $q = ab^{-1}$.• $R = \mathbb{Z}$, $N = |\cdot|$ Thm: $R = \mathbb{k}[x]$ is Euclidean if $N = \deg$, and moreover q and r are unique.Pf: $a(x) = 0 \Rightarrow q = r = 0$.

$$a(x) = \lambda \in \mathbb{k}^* \Rightarrow \begin{cases} q = 0 \text{ and } r = \lambda \text{ if } \deg b \geq 1 \\ q = \lambda b^{-1} \text{ and } r = 0 \text{ if } \deg b = 0. \end{cases}$$

 $\deg a = n \geq 1$: use induction.Let $a(x) = a_n x^n + \dots + a_0$ and $b(x) = b_m x^m + \dots + b_0$ with $a_n \neq 0 \neq b_m$. $m > n \Rightarrow q = 0$ and $r = a$ suffice. $m \leq n$: set $a' = a - \frac{a_n}{b_m} x^{n-m} b$. Then $\deg a' < n$, so

$$= q'b + r \quad \text{with } r = 0 \text{ or } \deg r < m.$$

Set $q = q' + \frac{a_n}{b_m} x^{n-m}$. Then $qb + r = (q' + \frac{a_n}{b_m} x^{n-m})b + r$

$$= q'b + r + \frac{a_n}{b_m} x^{n-m} b$$

$$= a - \frac{a_n}{b_m} x^{n-m} b + \frac{a_n}{b_m} x^{n-m} b$$

Why are q and r unique?

$$\left. \begin{aligned} a &= \hat{q}b + \hat{r} \text{ with } \hat{r} = 0 \text{ or } \deg \hat{r} < m \Rightarrow (\underbrace{\hat{q} - q}_\text{deg} b) = r - \hat{r} \text{ has } \deg < m \\ &= qb + r \end{aligned} \right\} \begin{aligned} \deg &= \deg(\hat{q} - q) + m \\ \text{if } \hat{q} - q &\neq 0 \end{aligned} \Rightarrow \hat{q} - q = 0$$

$$\Rightarrow r - \hat{r} = 0. \square$$

Lemma: R Euclidean domain \Rightarrow PID, and $I \subseteq R$ ideal $\Rightarrow I = \langle d \rangle$ for any $d \neq 0$ of minimal norm. 42

Pf: Fix such $d \in I$.

$$a \in I \Rightarrow a = qd + r \text{ with } r = a - qd \in I. \quad N(r) < N(d) \Rightarrow r = 0. \quad \square$$

Cor: $\mathbb{k}[x]$ is a PID and hence UFD.

Q. Is $\mathbb{k}[x, y]$? answer in a bit

Prop: R PID and $0 \neq p$ prime $\Rightarrow \langle p \rangle$ maximal.

Pf: $a \notin \langle p \rangle \Rightarrow \langle a, p \rangle = \langle d \rangle$ for some gcd of a and p ,
but $p \nmid d$ since $a \notin \langle p \rangle$. Unique factorization $\Rightarrow d \in R^*$.

So every ideal properly containing $\langle p \rangle$ is generated by a unit. \square

A. No: $R[y]$ PID $\Rightarrow R$ is a field because

$R[y]/\langle y \rangle \cong R$ is a domain $\Rightarrow \langle y \rangle$ is prime
 $\Rightarrow \langle y \rangle$ is maximal.

$\mathbb{k}[x, y] = \mathbb{k}[x][y]$ but $\mathbb{k}[x]$ is not a field.

Euclidean algorithm

Input: $a, b \in R$ with $b \neq 0$

Output: $\gcd(a, b)$

Init: q_0, r_0 with $a = q_0 b + r_0$ (0) q_1, r_1 $b = q_1 r_0 + r_1$ (1) $i = 1$ $r_0 = q_2 r_1 + r_2$ (2)	e.g. $\begin{array}{r} a \\ \hline b \\ \hline \end{array}$ $108 = 3 \cdot 30 + 18$ $30 = 1 \cdot 18 + 12$ $18 = 1 \cdot 12 + 6$ $12 = 2 \cdot 6$
--	---

While: $r_i \neq 0$

$$\text{Do: write } r_{i-1} = q_{i+1} r_i + r_{i+1} \quad r_0 = q_1 r_1 + r_2 \quad r_{n-3} = q_{n-1} r_{n-2} + r_{n-1} \quad (n-1)$$

$$i \leftarrow i+1 \quad r_{n-2} = q_n r_{n-1} + r_n \quad (n)$$

Return: r_{i-1} (call it r_n)

$$r_{n-1} = q_{n+1} r_n \quad (n+1)$$

Thm: $\langle a, b \rangle = \langle r_n \rangle$. that's the one you want.

Pf: (0) $\Rightarrow r_0 \in \langle a, b \rangle$. (1) $\Rightarrow r_1 \in \langle b, r_0 \rangle \subseteq \langle a, b \rangle$. (i) $\Rightarrow r_i \in \langle r_{i-2}, r_{i-1} \rangle \subseteq \langle a, b \rangle$ by induction.

(n+1) $\Rightarrow r_n \mid r_{n-1}$. (n) $\Rightarrow r_n \mid r_{n-2}$. (i) $\Rightarrow r_n \mid r_{i-2}$ for $i \geq 2$ by induction. on n-i

(1) $\Rightarrow r_n \mid b$. (0) $\Rightarrow r_n \mid a$. \square