Ex: $(\mathbb{Z}[X], +, \cdot)$ is factorial.

a) $P(X) = 3X^4 - 6X^3 - 9X^2 - 30X - 120$

$= 3(X^2+5)(X^2-2X-8)$

$= 3(X^2+5)(X+2)(X-4)$

b) $3X^3 - 3X^2 + 5X - 5$

$= (3X^2+5)(X-1)$

irreducible elements in $\mathbb{Z}[X]$.

The following definition should have been given before. For completeness we give it.

Def '99: Let A be an UFD. We consider the factor group $Q(A)^\times / A^\times$.

Given $a_0, \dots, a_d \in A$ (not all being 0_A) we have

$$\gcd(a_0, \dots, a_d) \in Q(A)^\times / A^\times.$$

Let $P \in Q(A)[X] \setminus \{0\}$, $P(X) = \sum_{i=0}^{d} \frac{a_i}{b_i} X^i$, $\frac{a_d}{b_d} \neq 0$.

Then $\exists\, a \in A \setminus \{0\}$ s.t. $aP \in A[X]$.

We call the class

$$\operatorname{cont}(P) := \left[\frac{1}{a}\right]_{A^\times} \cdot \left[\gcd(aa_0, \dots, aa_d)\right]$$

$$\in Q(A)^\times / A^\times$$

the content of P.

(Gauß) **Prop 100:** A a UFD, $P_1, P_2 \in Q(A)[X] \setminus \{0\}$

Then $\operatorname{cont}(P_1 P_2) = \operatorname{cont}(P_1)\operatorname{cont}(P_2)$

(an equation in $Q(A)^\times / A^\times$)

Proof: (exercise on the problem sheet) □

Example: 1) $A = \mathbb{Z}$

$$\operatorname{cont}(5X^4 + 15X^3 - 105X^2 + 80) = [5]_{\{\pm 1\}} = \{5, -5\}$$

$$\operatorname{cont}\left(\frac{7}{30}X^2 + \frac{28}{21}X - \frac{19}{105}\right) = \frac{1}{3}\cdot\frac{1}{5}\cdot\frac{1}{7}\cdot\frac{1}{13}.$$

↑ take min of the exponents for every prime number.

verify: $a := 3\cdot 5\cdot 7\cdot 13$

$$aP = \cancel{3\cdot 5\cdot 7^2\cdot 13}X^2 + 2^2\cancel{\cdot 3\cdot 5\cdot 7^2 13} \overset{*}{-} \cancel{3\cdot 5\cdot 7}\cdot 13\cdot 19$$

$$\operatorname{cont}(aP) = [1]_{\mathbb{Z}^\times} = \{\pm 1\}$$ □

2) A bit more artificial.

$A = \mathbb{C}[X]$ Consider $A[Y]$

$\mathrm{cont}_Y((X^2-9)Y + X^2 - 5X + 6)$

$= [X-3]_{A^\times} = [X-3]_{\mathbb{C}^\times}$

$\uparrow$ $A^\times = \mathbb{C}^\times$

$\in \mathbb{C}(X)^\times / A[X]^\times = \mathbb{C}(X)^\times / \mathbb{C}^\times$.

II.7 Euclidian rings

Here we consider integral domains where we can perform a Euclidian algorithm.
For that we need division with remainder. Here A is always an integral domain.

Def 101: A function $N: A \longrightarrow \mathbb{Z} \cup \{-\infty\}$ is called a Euclidian function if a) $N(A \setminus \{0\}) \subseteq \mathbb{Z}$ is bounded from below and

b) $N(0_A) \leq N(a) \quad \forall a \in A \setminus \{0\}$ and

c) $\forall a, b \in A$ with $b \neq 0$:

$\exists q, r \in A$ with $N(r) < N(b)$:

$$a = qb + r.$$

Def 102: An integral domain on which there exists a Euclidian function is called a Euclidian ring.

Examples:

1) $N: \mathbb{Z} \longrightarrow \mathbb{N}_0 \quad N(z) := |z|$
2) Let F be a field

$$N: F \longrightarrow \{0,1\} \quad N(a) := \begin{cases} 1, & a \neq 0 \\ 0, & a = 0. \end{cases}$$

3) $N: \mathbb{Q}[X] \longrightarrow \{-\infty\} \cup \mathbb{Z}$

$N(P) := \deg(P)$

(See Prop 7.6)

4) The following map is not a euclidian function.

$N: \mathbb{Q}[X,Y] \longrightarrow \{-\infty\} \cup \mathbb{Z}$.

$P \longmapsto \deg(P)$

$\deg(P) := \deg_{X,Y}(P)$

$$= \begin{cases} -\infty, & P = 0 \text{ polynomial} \\ \max\{i+j \mid i,j \in \mathbb{N}_0 \text{ s.t. coeff. of } P \text{ at } X^iY^j \text{ is non-zero}\} \end{cases}$$

Proof: $X + Y = q(X-Y) + r$

with $\deg(r) \leq 0$

Then $r = 0$, for $x = 0, y = 0$

$r = 2$, for $x = 1, y = -1$. ↯

□

A priori we did not require $N(ab) \geq N(b)$ $\forall a, b \in A \setminus \{0\}$

But this property can be achieved by a modification.

Prop 103: Let $\tilde{N}$ be an Euclidian function on A. Define

$$N(a) = \min_{b \in A \setminus \{0\}} \tilde{N}(ba) \qquad (*)$$

Then N is an Euclidian function.

Proof: • $\exists\, z_0 \in \mathbb{Z} : \forall a \in A \setminus \{0\} : \tilde{N}(a) \geq z_0 > \tilde{N}(0)$

$\Rightarrow N(a) = \min_{b \in A \setminus \{0\}} \tilde{N}(ba) \geq z_0 > N(0) = \tilde{N}(0)$

for all $a \in A \setminus \{0\}$

• Take $a, b \in A$ s.t. $b \neq 0$.

Then $\exists\, q_1 \in A$ and $r_1 \in A$ s.t.

$\tilde{N}(r_1) < \tilde{N}(b)$ and $a = q_1 b + r_1$

If $N(b) \leq \tilde{N}(r_1)$ then

$\exists\, c_1 \in A \setminus \{0\} : \tilde{N}(cb) \leq \tilde{N}(r_1)$

$\Rightarrow \exists\, q_2 \in A, r_2 \in A$ with $\tilde{N}(r_2) < \tilde{N}(bc)$

s.t. $r_1 = q_2 c_1 b + r_2$

So $a = (q_1 + q_2 c_1) b + r_2$

and $\tilde{N}(r_2) < \tilde{N}(cb) \leq \tilde{N}(r_1)$

Because $\tilde{N}(A \setminus \{0\})$ is bounded from below, this process has to stop after finitely many steps, i.e. we find $q \in A$ and $r \in A$ s.t. $\tilde{N}(r) < N(b)$ and $a = qb + r$
$\Rightarrow N(r) \leq \tilde{N}(r) < N(b)$. □

Prop 104: If an Euclidian function satisfies (*) then (q, r) in the division with remainder are uniquely determined.

Proof: $a \in A$, $b \in A \setminus \{0\}$.
Say $a = q_1 b + r_1 = q_2 b + r_2$
$\Rightarrow (q_1 - q_2) b = r_2 - r_1$
If $r_1 \neq r_2$ then $N(r_2 - r_1) = N((q_1 - q_2) b)$
$\overset{(*)}{\geq} N(b)$
$\Rightarrow \exists\, q \in A, r \in A \setminus \{0\}$ with $N(r) < N(b)$:
$r_2 - r_1 = q(q_1 - q_2) b + r$
$\Rightarrow r = (q_1 - q_2 - q) b$
$N(r) < N(b) \overset{(*)}{\Rightarrow} q_1 - q_2 - q = 0$
$\Rightarrow r = 0$

Examples:

$\mathbb{Z}[i]$ is an Euclidian ring.

Proof: $N(\alpha) := \alpha\bar{\alpha} = a^2+b^2$

if $\alpha = a+ib \in \mathbb{Z}[i]$.

$\Rightarrow \operatorname{im}(N) \subseteq \mathbb{N}_0 \setminus N(\mathbb{Z}[i]\setminus\{0\}) \subseteq \mathbb{N}$.

Take $\alpha = a+ib$.

and $\beta = c+id \neq 0$.

$\Rightarrow \quad \frac{\alpha}{\beta} \in \mathbb{Q}[i] \quad \frac{\alpha}{\beta} = e+if$

There are integers $z_r, z_i \in \mathbb{Z}$ s.t.

$|z_r - e| \leq \frac{1}{2}$ and $|z_i - f| \leq \frac{1}{2}$

Then $\alpha = q\beta + r$ with

$q := z_r + iz_i$ and

$r := \big((e-z_r) + i(f-z_i)\big)\beta$

and $N(r) \leq \frac{1}{2} \cdot N(\beta) < N(\beta)$ □

~~Prop 104: Euclidian rings are principal ideal domains (i.e. integral~~

Def 104: A non-zero commutative unitary ring R is called principal if every ideal is principal, i.e. generated by one element.

A principal integral domain is called a principal ideal domain (PID).

lecture 17

Prop 105: Every Euclidian ring is a PID and in particular factorial.

Proof: Let A be Euclidian with a Euclidian function $N: A \to \mathbb{Z} \cup \{\infty\}$. Take an ideal $(0) \neq \mathfrak{a} \subseteq A$ and an element $a \in \mathfrak{a} \setminus \{0\}$ s.t.

$$N(a) = \min_{b \in \mathfrak{a} \setminus \{0\}} N(b)$$

Claim: $(a)_A = \mathfrak{a}$.

$b \in \mathfrak{a} \Rightarrow \exists\, q, r \in A$ s.t. $N(r) < N(a)$:

$b = qa + r \Rightarrow r = b - qa \in \mathfrak{a}$

$\Rightarrow r = 0 \Rightarrow b \in (a)_A$ ☐

($\Uparrow$ $N(r) < N(a)$)

Ex: $\mathbb{Q}[X, Y]$ is not an Euclidian ring.

Proof: Claim: $(X, Y)_{\mathbb{Q}[X,Y]}$ is not principal.

Proof: Assume $\exists\, P \in \mathbb{Q}[X, Y]$:

$$(P)_{\mathbb{Q}[X,Y]} = (X, Y)_{\mathbb{Q}[X,Y]}.$$

Then $\exists\, R, S \in \mathbb{Q}[X, Y]$:

$X \overset{I}{=} RP$ and $Y \overset{II}{=} SP$

$\Rightarrow$ ~~$\deg_X P$~~ $R \in \mathbb{Q}^\times$ and $S \in \mathbb{Q}^\times$ because X and Y are irreducible.

Thus $\deg_Y P \overset{I}{=} 0$ and $\deg_Y P \overset{II}{=} 1$ ↯ ☐

☐

Prop 106: (Euclidian algorithm)
Let A be Euclidian and $a, b \in A$ s.t. $b \neq a$
Consider the following sequence $(q_i, r_i)_{i \geq 0}$

$$a = q_1 b + r_1 \qquad N(r_1) < N(b)$$
$$b = q_2 r_1 + r_2 \qquad N(r_2) < N(r_1)$$
$$r_1 = q_3 r_2 + r_3$$
$$\vdots$$
$$r_i = q_{i+2} r_{i+1} + r_{i+2} \qquad N(r_{i+2}) < N(r_{i+1})$$

as long as $r_{i+1} \neq 0$.

Then, there is an index $i_0 \in \mathbb{N}$ s.t. $r_{i_0} = 0$ and $r_{i_0 - 1} \in \gcd(a, b)$.
($r_{-1} := a$, $r_0 := b$)

Proof: We have $N(r_0) > N(r_1) > \dots$
and $N(A \setminus \{0\})$ is bounded ~~so~~ from below and $\subseteq \mathbb{Z}$.
So $\exists\, i_0 : r_{i_0} = 0$.
(If $z_0 \leq N(A \setminus \{0\})$, then
$[z_0, N(r_0)] \cap \mathbb{Z}$ is finite and
if there is no such i_0 s.t. $r_{i_0} = 0$
then $[z_0, N(r_0)] \cap \mathbb{Z}$ contains
infinitely many elements
$N(r_0), N(r_1), \dots$ ↯)

Let $t \in \gcd(a, b) \Rightarrow t \mid a$ and $t \mid b$
$\Rightarrow t \mid r_1 \Rightarrow t \mid r_2 \wedge t \mid r_1 \Rightarrow \dots \Rightarrow t \mid r_{i_0} \wedge t \mid r_{i_0 - 1}$
$t \mid e$