to be prepared for 7.12.2023

Exercise 28. Let R be a UFD and $f, g \in R[x]$ not both zero. Prove that

$$\gcd(f, g) \in R[x] \setminus R \iff \operatorname{res}(f, g) = 0.$$

Hint: Consider R as embedded in its quotient field and rewrite the vanishing of the resultant as a property of a (normalized) GCD.

Exercise 29. Prove the following theorem:

> Let $f, g \in \mathbb{F}[x, y]$, $\deg_x f = n$, $\deg_x g = m$, and $d \in \mathbb{N}$ s.t. $\deg_y f$, $\deg_y g \le d$. Then $\deg_y \operatorname{res}_x(fg) \le (n + m)d$.

Exercise 30. Prove the following theorem:

> Let $f, g \in \mathbb{Z}[x]$, $\deg f = n$, $\deg g = m$. Then
>
> $$|\operatorname{res}(f, g)| \le ||f||_2^m \, ||g||_2^n \le (n + 1)^{m/2}(m + 1)^{n/2}||f||_\infty^m ||g||_\infty^n.$$

Exercise 31. For application in modular algorithms we prove the following lemma:

Let R be a commutative ring with 1, $I \lhd R$ an ideal and $f, g \in R[x] \setminus 0$ s.t. $\overline{\operatorname{lc}(f)} \in R/I$ is not a zero divisor. Then

1. $\overline{\operatorname{res}(f, g)} = 0 \iff \operatorname{res}(\overline{f}, \overline{g}) = 0$.
2. If R/I is a UFD, then $\overline{\operatorname{res(f, g)}} = 0 \iff \gcd(\overline{f}, \overline{g}) \in \big(R/I\big)[x] \setminus \big(R/I\big)$ i.e., $\gcd(\overline{f}, \overline{g})$ is nonconstant.