to be prepared for 24.11.2022

Exercise 27. Let R be a UFD, $f, g \in R[x]$ and $h = \mathrm{GCD}_{R[x]}(f, g)$. Prove that

1. $\mathrm{cont}(h) = \mathrm{gcd}_R\big(\mathrm{cont}(f), \mathrm{cont}(g)\big)$ and $\mathrm{pp}(h) = \mathrm{GCD}_{R[x]}\big(\mathrm{pp}(f), \mathrm{pp}(g)\big)$;
2. $h = \mathrm{gcd}_R\big(\mathrm{cont}(f), \mathrm{cont}(g)\big) \cdot \mathrm{GCD}_{R[x]}\big(\mathrm{pp}(f), \mathrm{pp}(g)\big)$;
3. If f or g is primitive then so is h.

Exercise 28. Prove the following statement for univariate polynomials:

Let $f, g \in \mathbb{F}[x]$ where $\mathbb{F}$ denotes a field. Then

$$\gcd(f, g) \neq 1 \iff \exists_{s,t\in\mathbb{F}[x]\setminus 0} \big(sf + tg = 0 \wedge \deg s < \deg g \wedge \deg t < \deg f\big).$$

Exercise 29. Let $f, g \in \mathbb{F}[x] \setminus 0$ with $\deg f = n$, $\deg g = m$. Consider the map

$$\varphi\colon \mathbb{F}[x]_{<m} \times \mathbb{F}[x]_{<n} \to \mathbb{F}[x]_{<m+n},\ \varphi(s, t) = sf + tg.$$

Write down those (ordered) $\mathbb{F}$-bases of $\mathbb{F}[x]_{<m} \times \mathbb{F}[x]_{<n}$ and of $\mathbb{F}[x]_{<m+n}$ so that the Sylvester matrix $\mathrm{Syl}(f, g)$ (in the version that is introduced in the lecture) is indeed the matrix of φ.

Exercise 30. Let R be a UFD and $f, g \in R[x]$ not both zero. Prove that

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

Hint: Take R as embedded in its quotient field $\mathbb{F} = Q(R)$ and note that there is a commutative diagram

$$\begin{array}{ccc} \mathbb{F}[x] \times \mathbb{F}[x] & \xrightarrow{\mathrm{res}} & \mathbb{F} \\ \uparrow & & \uparrow \\ R[x] \times R[x] & \xrightarrow{\mathrm{res}} & R \end{array}$$

Thus, $\mathrm{res}(f, g)$ is an element of R, no matter whether the resultant is taken over R or over $\mathbb{F}$. Now reformulate the vanishing of the resultant as a property of a (normalized) GCD.

Exercise 31. Let R be an integral domain, $f, g \in R[x] \setminus 0$. Prove that there are polynomials $s, t \in R[x]$ with $\deg s < \deg g$ and $\deg t < \deg f$ such that $\mathrm{res}(f, g) = sf + tg$. Show that s and t are unique in case that $\mathrm{res}(f, g) \neq 0$.

Hint: You may use Linear Algebra to find a desired representation over the quotient field of R. Then demonstrate that s and t are in $R[x]$.

Exercise 32. Let R be a commutative ring with 1, $I \lhd R$ an ideal and denote the value of a polynomial h under the surjective ring homomorphism $R[x] \to R/I\,[x]$ by $\overline{h}$, i.e., if $h = \sum_{k=0}^{n} h_k x^k$, then

$$\overline{h} = \sum_{k=0}^{n} (h_k + I)\, x^k.$$

Note that this map is an extension of the canonical epimorphism $R \to R/I$ so that the same notation applies to ring elements $c \in R$ (considered as constant polynomials).

Let $f, g \in R[x] \setminus 0$ and assume that $\overline{\mathrm{lc}(f)}$ is not a zero divisor in R/I. Show that

$$\overline{\mathrm{res}(f, g)} = 0 \iff \mathrm{res}\big(\overline{f}, \overline{g}\big) = 0.$$