to be prepared for 14.12.2023

Exercise 32. Prove the following statement (part of the GCD-Theorem):

> Let R be an ED, $f, g \in R[x]^\star$ and $p \in R$ a prime with $p \not| \operatorname{gcd}_R\big(\operatorname{lc}(f), \operatorname{lc}(g)\big)$; let $\mathbb{F} = R/\langle p\rangle$ be its quotient field. Then the following are equivalent:
>
> 1. $\deg\Big(\operatorname{gcd}_{\mathbb{F}[x]}\big(\overline{f}, \overline{g}\big)\Big) = \deg\big(\operatorname{gcd}_{R[x]}(f, g)\big)$;
> 2. $\overline{\operatorname{lc}\big(\operatorname{gcd}_{R[x]}(f,g)\big)} \cdot \operatorname{gcd}_{\mathbb{F}[x]}(\overline{f}, \overline{g}) = \overline{\operatorname{gcd}_{R[x]}(f,g)}$;
> 3. $p \not|_R \operatorname{res}\Big(\frac{f}{\operatorname{gcd}_{R[x]}(f,g)}, \frac{g}{\operatorname{gcd}_{R[x]}(f,g)}\Big)$.

Exercise 33. Let $<$ be a relation on $\mathbb{N}^n$.

Prove the equivalence of the following definitions of a monomial order.

1. $<$ is a well-order and $\forall_{\alpha,\beta,\gamma\in\mathbb{N}^n}\ \big(\alpha < \beta \Rightarrow \alpha + \gamma < \beta + \gamma\big)$;
2. $<$ is a total order and $\forall_{\alpha\in\mathbb{N}^n}\ 0 \leq \alpha$ and $\forall_{\alpha,\beta,\gamma\in\mathbb{N}^n}\ \big(\alpha < \beta \Rightarrow \alpha+\gamma < \beta+\gamma\big)$.

Exercise 34. Prove that $<_{\text{lex}}$, $<_{\text{grlex}}$ and $<_{\text{grevlex}}$ are monomial orders in $\mathbb{N}^n$.

Exercise 35. Consider the polynomial $f = 2xy^2 - xy + x^3$ in the ring $K[x, y]$. Find monomial orders $<_1$ and $<_2$ so that $\operatorname{lm}_{<_1}(f) \neq \operatorname{lm}_{<_2}(f)$.

Exercise 36. Let R be a commutative ring with 1. Prove the equivalence of the following statements.

1. Every ideal in R has a finite basis.
2. Each non empty set of ideals has an element that is maximal with respect to inclusion.
3. Each increasing chain of ideals terminates, i.e., if $M_1 \subseteq M_2 \subseteq \cdots$ is an ascending chain of ideals then there is an $N \in \mathbb{N}$ s.t. $\forall n \geq N\ M_n = M_N$.

Note that this is true for submodules of a module over an arbitrary ring.