

1. For the first item you can use a lemma on antichains, but it has to be formulated.
 - (a) Prove that a monomial ideal is finitely generated.
 - (b) Prove that every ideal of $k[x_1, \dots, x_n]$ can be generated by a finite number of elements.
 - (c) Prove that every ideal of $k[x_1, \dots, x_n]$ has a finite Gröbner basis.
2. Let $f, g \in k[x_1, \dots, x_n]$. Suppose that the least common multiple of $\text{LM}(f)$ and $\text{LM}(g)$ is the product $\text{LM}(f)\text{LM}(g)$. Prove that $S(f, g)$ reduces to 0 modulo $\{f, g\}$.
3. Let $I \subset k[x_1, \dots, x_n]$ be an ideal, and G a Gröbner basis of I with respect to the lexicographic order, where $x_1 >_{\text{lex}} x_2 > \dots >_{\text{lex}} x_n$. Let $I_l = I \cap k[x_{l+1}, \dots, x_n]$. Show that $G \cap k[x_{l+1}, \dots, x_n]$ is a Gröbner basis of I_l .

4. Let k be a field and $T_1, \dots, T_n \subset k$ finite subsets. Set $t_i = |T_i|$, $T = T_1 \times \dots \times T_n \subset k^n$, and

$$I(T) = \{f \in k[x_1, \dots, x_n] \mid f(p) = 0 \text{ per ogni } p \in T\}.$$

Let

$$f_i(x_i) = \prod_{s \in T_i} (x_i - s).$$

Prove that f_1, \dots, f_n is a Gröbner basis of $I(T)$, with respect to any monomial order.

5. (a) Let $x \in \mathbb{R}$, $x > 1$. Let $\frac{b_i}{c_i}$ be the convergents of the continued fraction of x . Show that $|b_i^2 - c_i^2 x^2| < 2x$.
 - (b) In what way is this result being used in the continued fractions method for factorising an integer n ?
6. Let $f \in \mathbb{F}_q[x]$. Let $v \in \mathbb{F}_q[x]$ be such that $v^q \equiv v \pmod{f}$. Show that

$$f = \prod_{a \in \mathbb{F}_q} \text{mcd}(f, v - a).$$

7. Let q be a power of an odd prime. Let $\gamma \in \mathbb{F}_q^*$. It is known that $\gamma^{\frac{q-1}{2}} = 1$ if and only if γ is a square and $\gamma^{\frac{q-1}{2}} = -1$ if and only if γ is not a square. Describe a probabilistic method for factorising polynomials in $\mathbb{F}_q[x]$, based on this fact.
8. Let $f \in \mathbb{Z}[x]$ and p a prime. Let $g, h \in \mathbb{Z}[x]$ with
 - $\deg(g) + \deg(h) = \deg(f)$,
 - $\gcd(h, g) = 1 \pmod{p}$,
 - $f = gh \pmod{p^k}$ (for a certain $k > 0$).

Show that there exist $\tilde{g}, \tilde{h} \in \mathbb{Z}[x]$ with

- $\deg(\tilde{g}) = \deg(g)$, $\deg(\tilde{h}) = \deg(h)$,
- $\tilde{g} = g \pmod{p^k}$, $\tilde{h} = h \pmod{p^k}$,
- $f = \tilde{g}\tilde{h} \pmod{p^{k+1}}$.

Show how the proof gives a method for finding \tilde{g} , \tilde{h} .