Name: .... 27 Jan 2017

Studienkennzahl: ....

Matrikelnummer: ....

Final Exam / Klausur
Computer Algebra (326.010)
(no books / ohne Unterlagen)

You may give answers either in English or in German.
Man kann auf Englisch oder Deutsch antworten.

Explain your answers. Simply giving the result or "yes/no" is not enough.
Antworten sind zu begründen. Nur das Ergebnis oder "ja/nein" genügt nicht.

(1) Consider the following polynomials in $\mathbb{Z}_5[x]$:

$$a(x) = x^5 + 2x^3 + 4x^2 + 3 \ , \quad b(x) = 2x^4 + x^3 + 2x + 2 \ .$$

(a) Determine the greatest common divisor c of a and b.
(b) What is the normed reduced Gröbner basis of the ideal $\langle a, b\rangle$?

(2) Consider the following polynomials in $\mathbb{Q}[x]$ with undetermined coefficients:

$$a(x) = a_2x^2 + a_1x + a_0 \ , \quad b(x) = b_1x + b_0 \ .$$

If a and b have a common solution, the coefficients of a and b have to satisfy a certain polynomial relation.
What is this polynomial relation?
[Hint: think of the resultant]

(3) (a) Give a definition of the **Chinese Remainder Problem (CRP)** in $\mathbb{Z}$.
(b) Solve the following CRP in $\mathbb{Z}$:

$$r \equiv 1 \bmod 3 \ , \ r \equiv 2 \bmod 5 \ , \ r \equiv 3 \bmod 7 \ .$$

(4) Let K be a field.
(a) Give a definition of an **ideal** in $K[x_1, \ldots, x_n]$, and of a **basis** of an ideal.
(b) Does every ideal in $K[x_1, \ldots, x_n]$ have a finite basis? Do you know the name of a theorem which answers this question?
(c) Give a definition of the **membership problem** for ideals in $K[x_1, \ldots, x_n]$.

(5) Consider the polynomial ring $K[x_1, \ldots, x_n]$, K a field.
(a) Let G be a Gröbner basis w.r.t. $<$ for the ideal I. Let $g, h \in G$ such that $g \neq h$.
Prove:
If the leading power product of g divides the leading power product of h, then $G' = G \setminus \{h\}$ is also a Gröbner basis w.r.t. $<$ of I.
(b) Give definitions of the following notions:
– minimal Gröbner basis,
– reduced Gröbner basis,
– normed Gröbner basis.