Name: .... 28 Jan 2014

Studienkennzahl: ....

Matrikelnummer: ....

Final Exam
Computer Algebra (326.010)
(no books allowed)

(1) Let D be a Euclidean domain (such as $\mathbb{Z}$, or $\mathbb{Q}[x]$). Let p be an irreducible element of D, and a a non-zero element of D.
  (i) Explain how you could compute a^{-1} in D modulo p; i.e. an element b such that the remainder on division of $a \cdot b$ by p is 1.
  (ii) Determine 35^{-1} in $\mathbb{Z}_{73}$;
  (iii) Determine $(x+1)^{-1}$ in $\mathbb{Q}[x]$ modulo x^2+2.

(2) **Theorem 4.1.** (lecture notes computer algebra)
Let $a(x), b(x)$ be two non-constant polynomials in $K[x]$, K a field. Then a and b have a non-constant common factor (i.e. a common root over the algebraic closure of K) if and only if there are polynomials $p(x), q(x) \in K[x]$, not both equal to 0, with $\deg(p) < \deg(b), \deg(q) < \deg(a)$, *such that* $p(x)a(x) + q(x)b(x) = 0$.
Based on Theorem 4.1, determine the formula for the Sylvester matrix of a and b.

(3) Consider the following polynomials in $\mathbb{Q}[x, y]$:

$$a(x, y) = xy^2 + 2y^2 - xy - 2, \qquad b(x, y) = xy + 2y + x - 4$$

  (i) Compute $\mathrm{res}_y(a, b) \in \mathbb{Q}[x]$, the resultant of a and b w.r.t. y;
  (ii) Can the solution $x = -2$ of $\mathrm{res}_y(a, b)$ be extended to a solution of the system $a(x, y) = 0 = b(x, y)$? Explain this situation.
  (iii) Can the solution $x = 1$ of $\mathrm{res}_y(a, b)$ be extended to a solution of the system $a(x, y) = 0 = b(x, y)$? Explain this situation.

(4) Prove: *If $f, g \in \mathbb{Q}[x, y]$ are relatively prime (i.e. $\gcd(f, g) = 1$), then there are only finitely many pairs $(a, b) \in \mathbb{C}^2$ such that $f(a, b) = 0 = g(a, b)$.*
[Hint: consider the gcd of f and g in $\mathbb{Q}(x)[y]$.]

(5) Consider the polynomials $a(x, y)$ and $b(x, y)$ of Question (3). The system $a(x, y) = b(x, y) = 0$ has 2 roots in $\mathbb{C}^2$. We want to determine a Gröbner basis G for the ideal generated by $\{a, b\}$ w.r.t. the lexicographic order with $x < y$:
  $\mathrm{spol}(a, b)$ can be reduced to $2(4y + x - 5)$, so we add $c = 4y + x - 5$ to the basis;
  $\mathrm{spol}(a, c)$ can be reduced to $\frac{1}{4}(x^2 - 7x + 6)$, so we add $d = x^2 - 7x + 6$ to the basis;
Complete the algorithm and determine G.