Name: .... 30 Jan 2007

Studienkennzahl: ....

Matrikelnummer: ....

Final Exam
Computer Algebra (326.017)

(1) Consider the ring $R := \mathbb{Z}[\sqrt{-3}] = \{a + b\sqrt{-3} \mid a, b \in \mathbb{Z}\}$ (a subring of $\mathbb{C}$) with the usual addition and multiplication. Moreover, consider the function $\phi(a + b\sqrt{-3}) = a^2 + 3b^2$ from R into $\mathbb{N}$. Show:
(i) $\phi(u \cdot v) = \phi(u) \cdot \phi(v)$;
(ii) R is an integral domain;
(iii) the elements $2, 1 \pm \sqrt{-3}$ are irreducible;
(iv) R ist <u>not</u> a unique factorization domain.

(2) Suppose $f(x, y) \in \mathbb{Q}[x, y]$ has the irreducible factors f_i with multiplicities e_i, i.e.

$$f(x,y) = \prod_{i=1}^{r} f_i(x,y)^{e_i} \ .$$

(i) Show that

$$\gcd(f, \frac{\partial f}{\partial x}, \frac{\partial f}{\partial y}) \ = \ \prod_{i=1}^{r} f_i(x,y)^{e_i - 1} \ .$$

(ii) How can one test whether a polynomial in $\mathbb{Q}[x, y]$ is square-free?

(3) Prove Fermat's Little Theorem, i.e.: *If p is a prime number and $\mathbb{Z}_p$ is the field with p elements, then for every non-zero $a \in \mathbb{Z}_p$ (so $a \neq 0$) we have $a^{p-1} = 1$.*

(4) (i) Prove that $x^2 + x + 2$ is irreducible in $\mathbb{Z}_3[x]$.
(ii) Construct explicitly the finite field with 9 elements.

(5) (i) Let R be a commutative ring with identity 1. What is an ideal in R?
(ii) A commutative ring with 1 is **Noetherian** iff there is no infinite strictly increasing chain of ideals of the form $I_1 \subset I_2 \subset \cdots \subset R$.
Give an example of a non-Noetherian commutative ring with 1.

(6) Let $a(x) = a_2x^2 + a_1x + a_0$ and $b(x) = b_2x^2 + b_1x + b_0$ be quadratic polynomials over a field K. Let $c(x) = c_1x + c_0$ (with $c_1 \neq 0$) be the remainder on division of a by b, i.e. $c(x) = \mathrm{rem}(a, b)$. Prove:

$$\mathrm{resultant}_x(a,b) \ = \ b_2 \cdot \mathrm{resultant}_x(c,b) \ .$$

(Hint: Consider the corresponding Sylvester matrices. Relate division of polynomials to elementary row operations on the Sylvester matrix.)