max planck institut informatik

SAARLAND UNIVERSITY
COMPUTER SCIENCE

Michael Sagraloff **Winter term 2017/18**

Computer Algebra

https://www.mpi-inf.mpg.de/departments/algorithms-complexity/teaching/winter17/comp-alg/

Assignment sheet 6 due: Monday, December 4

Exercise 1: Irreducibility vs. primality (4 points)

- Let R be an integral domain. Prove that if $p \in R$ is prime, then p is also irreducible:

$$p \in R \text{ is prime} \Rightarrow p \text{ is irreducible.}$$

  Give an example, where the other direction is wrong.

- Let R be a principal ideal domain. Prove that, in this situation, equivalence holds:

$$p \in R \text{ is prime} \Leftrightarrow p \text{ is irreducible.}$$

Exercise 2: Properties of rings (4 points)

1. Show that $\mathbb{Z}[x]$ is not a principal ideal domain.
2. Give an example of an irreducible element in the ring $\mathbb{Z}[\sqrt{-13}]$ that is not prime.
3. Give an example of a (non-factorial) ring R in which Gauß' Lemma does not hold; that is, there is a polynomial $f \in R[x]$, which is irreducible over $R[x]$, but factors over $F[x]$, where F is the quotient field of R.

Exercise 3: Euclidean Domains

1. Prove: If R is a Euclidean domain, then R is also a principal ideal domain.
2. Show that $\mathbb{Q}[x_1, \ldots, x_n]$ is not a Euclidean domain for all $n \geq 2$.

Exercise 4: GCD of Integers (4 points)

Show that, for two integers $a, b \in \mathbb{Z}$ of length less than L, the Euclidean algorithm uses $O(L)$ iterations. Further show that this bound is optimal, and derive a bound on the bit complexity of the Euclidean algorithm!

Hint: Show first that $r_{i-1} > 2 \cdot r_{i+1}$, where r_i is the remainder obtained in the i-th iteration of the algorithm.