Algebraic Algorithms

mykyta.narusevych@matfyz.cuni.cz

December 2022

1 Theoretical part

1. Compute square-free factorization of the polynomial
   $x^7 + x^6 - x^5 - x^4 - x^3 - x^2 + x + 1$ over $\mathbb{Z}[x]$.

2. Compute square-free factorization of the polynomial
   $x^{10} + 2x^9 + 2x^8 + 2x^7 + x^6 + x^5 + 2x^4 + x^3 + x^2 + 2x + 1$ over $\mathbb{Z}[x]$.

3. Compute square-free factorization of the polynomial
   $x^6 + x^4 + x^2 + 1$ over $\mathbb{Z}_2[x]$.

4. Compute square-free factorization of the polynomial
   $x^7 + x^6 + x^4 + x^3 + x + 1$ over $\mathbb{Z}_3[x]$.

5. Let $\mathbf{R}$ be gaussian field with characteristic 0 and let f be a primitive polynomial from $\mathbf{R}[x_1, ..., x_m]$. Prove that:

   - f is square-free iff $\gcd(f, \frac{\partial f}{\partial x_1}, ..., \frac{\partial f}{\partial x_m}) = 1$;
   - if $f = \prod_{i=1}^{k} h_i^i$ is a square-free decomposition, then

   $$\gcd(f, \frac{\partial f}{\partial x_1}, ..., \frac{\partial f}{\partial x_m}) = \prod_{i=1}^{k} h_i^{i-1}.$$

   Applying this proposition design an algorithm for square-free factorization of multivariate polynomials over gaussian rings with 0 characteristic.

2 Computational part

1. Verify 1 using sage.
2. Verify 2 using sage.
3. Verify 3 using sage.
4. Verify 4 using sage.