Classical Algebra

Written Assignment No. 5

due Thursday, December 4, 2008

Directions

Written assignments must be typeset.

While it is neither necessary nor desirable to show small details of computation, you must indicate what you are doing, give major steps in computation, and explain any reasoning used.

Accuracy is important. With 5 problems in an assignment worth 10 points, there is limited room for partial credit on a problem.

Problems

1. (1 point) Find the monic greatest common divisor over the finite field $\mathbf{F}_5$ of the two polynomials
$$x^4 - 1 \quad \text{and} \quad x^4 + 3x^2 + 1 \quad .$$

2. (1 point) The monic greatest common divisor of the polynomials
$$f(x) \;=\; x^5 - x - 1 \quad \text{and} \quad g(x) \;=\; x^3 + x + 1 \;,$$
regarded as polynomials with rational coefficients, is the constant polynomial 1. Express 1 as a polynomial linear combination of f and g. (Be sure to verify the correctness of your answer by expanding the linear combination.)

3. Find the order of the congruence class of the polynomial $f(x)$ modulo the polynomial $m(x)$ when the field of coefficents is $\mathbf{F}_p$ in the following cases:
   (a) (1 point) $f(x) = x$, $m(x) = x^2 + 1$, and $p = 7$.
   (b) (1 point) $f(x) = x$, $m(x) = x^2 - x + 2$, and $p = 5$.
   (c) (1 point) $f(x) = x - 1$, $m(x) = x^2 - x + 5$, and $p = 7$.

4. (1 point) Find a polynomial $f(t)$ in $\mathbf{F}_5[t]$ whose congruence class modulo $m(t)$ is a primitive element for the field $\mathbf{F}_5[t]/m(t)\mathbf{F}_5[t]$ when $m(t) = t^2 - t + 2$.

5. (1 point) Write a proof of the following proposition: If F is a field and $f(t)$ is in the ring $F[t]$ of polynomials with coefficients in F, then the polynomial t and the polynomial $f(t)$ have no (non-constant) common factor if and only if $f(0) \neq 0$.

6. $\mathbf{F}_4$ is defined to be the field $\mathbf{F}_2[t]/(t^2 + t + 1)\mathbf{F}_2[t]$.
   (a) (1 point) How many congruence classes are there of polynomials in $\mathbf{F}_4[x]$ modulo the polynomial $x^3 + x^2 + 1$?
   (b) (1 point) Explain why the polynomial $x^3 + x^2 + 1$ is irreducible over $\mathbf{F}_4$.
   (c) (1 point) Find a primitive element for the ring $\mathbf{F}_4[x]/(x^3+x^2+1)\mathbf{F}_4[x]$ of congruence classes.