Classical Algebra (Math 326)

Written Assignment No. 5

due Monday, Dec 8, 2003

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 and explain any reasoning used. Accuracy is important; with 5 problems in an assignment worth 5 points, there will be no room for partial credit on a problem.
Explain your solutions.

If you are in the writing intensive division of the course, you must complete each written assignment in a satisfactory way. This may require re-submission after an initial evaluation.

Problems

1. 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) $f(x) = x$, $m(x) = x^2 + 1$, and $p = 5$.
   (b) $f(x) = x$, $m(x) = x^2 - x + 1$, and $p = 5$.
   (c) $f(x) = x - 2$, $m(x) = x^2 + 5x + 1$, and $p = 7$.
   (d) $f(x) = x + 1$, $m(x) = x^3 - x^2 + 1$, and $p = 3$.
2. 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 $m(t) = t^2 - t + 1$.
3. $\mathbf{F}_4$ is defined to be the field $\mathbf{F}_2[t]/(t^2 + t + 1)\mathbf{F}_2[t]$.
   (a) How many congruence classes are there of polynomials in $\mathbf{F}_4[x]$ modulo the polynomial $x^3 + x + 1$?
   (b) Find a primitive element for the ring $\mathbf{F}_4[x]/(x^3 + x + 1)\mathbf{F}_4[x]$ of congruence classes.
   (c) Explain why the polynomial $x^3 + x + 1$ is irreducible over $\mathbf{F}_4$.
4. Let $f(t)$ be a polynomial of degree 5 over $\mathbf{F}_2$.
   (a) List three irreducible polynomials in $\mathbf{F}_2[t]$ of degree smaller than 5 having the property that f is irreducible if it is divisible by none of them.
   (b) Give an example of a polynomial f of degree 5 that is not divisible by any of the three polynomials you listed for the previous part.
   (c) For the polynomial $f(t)$ given in the previous part find a polynomial $g(t)$ in $\mathbf{F}_2[t]$ of smallest possible degree such that $g(t)$ is primitive in the field $\mathbf{F}_2[t]/f(t)\mathbf{F}_2[t]$.
5. 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 $f(0) \neq 0$.