Math 75 – Homework #2
posted April 4, 2008; due Monday, April 7, 2008

Exercises

1. Suppose F is a field, $f \in F[x]$ and $\beta \in F$. Show that $x - \beta \mid f(x)$ in $F[x]$ if and only if $f(\beta) = 0$.

2. Suppose F is a field, $f \in F[x]$ and $\deg(f) = d$. Show that f has at most d roots in F.

3. Show that the last exercise need not hold if F is not a field, by considering the nonfield $R = \mathbf{Z}/(8)$ and the polynomial $x^2 - 1$ in $R[x]$.

4. Let $F = \mathbf{Z}/(2)$. Find all irreducible polynomials in $F[x]$ of degrees 1, 2, 3, and 4.

5. Construct a finite field with 9 elements, by using the polynomial $x^2 + 1 \in (\mathbf{Z}/(3))[x]$. Write a multiplication table for the field.

6. In a finite group G with operation $\circ$, the *order* of an element g is the least positive integer k for which $g \circ g \circ \cdots \circ g$ (with k factors of g here) is the group identity. For example, in the additive group $\mathbf{Z}/(6)$, the order of 1 is 6, the order of 2 is 3, the order of 4 is also 3, etc. Another example: in the multiplicative group of the finite field $\mathbf{Z}/(5)$, the order of 1 is 1, the order of 2 is 4, etc. In the multiplicative group of the finite field with 9 elements that you constructed in the previous exercise, find the order of each of the 8 elements.

7. Show that every finite field K with 4 elements is *isomorphic* to $F[x]/(x^2 + x + 1)$, where $F = \mathbf{Z}/(2)$. In other words, it is possible to relabel the elements of K with the symbols '$[0]$', '$[1]$', '$[x]$', '$[x+1]$' to make the addition and multiplication tables in K simultaneously coincide with the addition and multiplication tables for $F[x]/(x^2 + x + 1)$, shown on the next page.

8. Let p be a prime, and let $F = \mathbf{Z}/(p)$. We have seen that in $F[x]$ we have the identity
$$x^p - x = x(x-1)(x-2)\cdots(x-(p-1)).$$
Use this to prove *Wilson's theorem* from elementary number theory:
$$1 \cdot 2 \cdot 3 \cdots (p-1) = -1 \quad \text{in } \mathbf{Z}/(p).$$

$+$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[0]$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[1]$	$[1]$	$[0]$	$[x+1]$	$[x]$
$[x]$	$[x]$	$[x+1]$	$[0]$	$[1]$
$[x+1]$	$[x+1]$	$[x]$	$[1]$	$[0]$

Table 1: Addition table for $F[x]/(x^2+x+1)$, where $F = \mathbf{Z}/(2)$.

$\cdot$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[x]$	$[x+1]$
$[x]$	$[0]$	$[x]$	$[x+1]$	$[1]$
$[x+1]$	$[0]$	$[x+1]$	$[1]$	$[x]$

Table 2: Multiplication table for $F[x]/(x^2+x+1)$, where $F = \mathbf{Z}/(2)$.