Groups and Rings - SF2729

Homework 2 (Rings)

Jim Holmström - 890503-7571

April 15, 2012

Exercise 1. Let $\sigma_m : \mathbb{Z} \to \mathbb{Z}_m$ be the natural homomorphism given by $\sigma_m(a) = a\ (mod\ m)$.

a. Show that $\overline{\sigma_m} : \mathbb{Z}[x] \to \mathbb{Z}_m[x]$ given by

$$\overline{\sigma_m}(a_0 + a_1 x + \ldots + a_n x^n) = \sigma_m(a_0) + \sigma_m(a_1)x + \ldots + \sigma_m(a_n)x^n \tag{1}$$

is an homomorphism of $\mathbb{Z}[x]$ onto $\mathbb{Z}_m[x]$.

b. Show that $degree(f(x) \in \mathbb{Z}[x]) = degree(\overline{\sigma_m}(f(x))) = n \bigwedge \overline{\sigma_m(f(x))}$ has no nontrivial factors in $\mathbb{Z}_m[x] \Rightarrow f(x)$ is irreducible in $\mathbb{Q}[x]$.

c. Show that $x^3 + 17x + 36$ is irreducible in $\mathbb{Q}[x]$

Solution. a. $\overline{\sigma_m}(f(x)+g(x)) = \overline{\sigma_m}\sum(f_i + g_i)x^i = \sum \overline{\sigma_m}(f_i + g_i)x^i = \sum(\overline{\sigma_m}(f_i) + \overline{\sigma_m}(g_i))x^i = \overline{\sigma_m}(f(x)) + \overline{\sigma_m}(g(x))$ and $\overline{\sigma_m}(f(x)g(x)) = \overline{\sigma_m}\left(\sum\left(\sum f_i g_{n-i}\right)x^n\right) = \sum \overline{\sigma_m}\left(\sum f_i g_{n-i}\right)x^n = \sum\left(\sum \overline{\sigma_m}(f_i g_{n-i})\right)x^n = \sum\left(\sum \overline{\sigma_m}(f_i)\overline{\sigma_m}(g_{n-i})\right)x^n = \overline{\sigma_m}(f(x))\overline{\sigma_m}(g(x))$ Which shows that $\overline{\sigma_m}$ is an homomorphism.
$a(x) \in \mathbb{Z}_m[x]$ and $b(x) \in \mathbb{Z}[x]$ having the same coeffs but seen as in $\mathbb{Z}$instead of $\mathbb{Z}_m$ with this we see that $\overline{\sigma_m}(a(x)) = b(x)$, so it is onto. □

b. $f = gh$ for $g, h \in \mathbb{Z}[x]$ where $degree(f) > degree(g) \wedge degree(f) > degree(h)$
Applying $\overline{\sigma_m}$ on f: $\overline{\sigma_m}(f) = \overline{\sigma_m}(g)\overline{\sigma_m}(h)$ is a factorization of $\overline{\sigma_m}$ into polynoms with a degree less then n of $\overline{\sigma_m}(f)$ which is a contradiction
$\Rightarrow f(x)$ is irreducible in $\mathbb{Z}[x]$
$\Rightarrow$ (by Theorem 23.11) $f(x)$ is irreducible in $\mathbb{Q}[x]$ □

c. Magically choosing $m = 5$
$\overline{\sigma_5}(x^3 + 17x + 36) = x^3 + 2x + 1$
By hand it's simple to show that:

$$(x^3 + 2x + 1)(\{-2, -1, 0, 1, 2\}) \neq 0 \tag{2}$$

and by Theorem 23.10 irreducible over $\mathbb{Z}_5$ and by the findings in (b) we also have that $x^3 + 17x + 36$ is irreducible over $\mathbb{Q}$ □

Exercise 2. Let $f(X) = X^4 - X^2 + 1$. Prove that $f(X)$ is irreducible in $\mathbb{Z}[X]$ and show that $f(X)$ is reducible in $\mathbb{Z}_m[X]$ for $m = \{2, 3, 5\}$ by determining the factorization into a product of irreducible polynomials.

Solution.