MATH 503: HOMEWORK #2A

DUE FRIDAY, FEB. 8 IN YING’S MAILBOX

1. IRREDUCIBILITY

1. Show that the polynomial $x^4+1$ is irreducible in $\mathbb{Z}[x]$. (Hint: Try using Eisenstein’s criterion with $p = 2$ after a simple change of variable.) The problems below will lead to a proof that $x^4 + 1$ is reducible in $(\mathbb{Z}/p)[x]$ for all primes $p$.

2. Check that $x^4 + 1$ is reducible in $(\mathbb{Z}/2)[x]$. (Hints: Look for a root in $\mathbb{Z}/2$.)

3. Suppose $p > 2$ is a prime. Show that in $(\mathbb{Z}/p)[x]$, the polynomial $x^4 + 1$ divides $x^{p^2-1} - 1$ and thus also $x^{p^2} - x$. (Hints: $x^4 + 1$ divides $x^8 - 1$, and $p^2 \equiv 1 \mod 8$.)

4. Show that if $f(x)$ is a monic irreducible polynomial of degree 1 or 2 in $(\mathbb{Z}/p)[x]$ then $f(x)$ divides $x^{p^2} - x$ in $(\mathbb{Z}/p)[x]$.

(Hints: Explain why $L = \frac{(\mathbb{Z}/p)[x]}{(\mathbb{Z}/p)[x] \cdot f(x)}$ is a field having either $p$ or $p^2$ elements. The multiplicative group $L^* = L - \{0\}$ has order $p - 1$ or $p^2 - 1$. If $f(x) \neq x$, show that the image $[x]$ of $x$ in $L$ is an element of $L^*$ which has order dividing the order of $L^*$. Explain why this leads to $x^{p^2-1} - 1 \equiv 0 \mod (\mathbb{Z}/p)[x] \cdot f(x)$ if $f(x) \neq x$. Now treat the case $f(x) = x$.)

5. Count the number of monic irreducible $f(x)$ in $(\mathbb{Z}/p)[x]$ which have degrees 1 and 2. (Hint: The $f(x)$ of degree 1 are easy to count. For those of degree 2, first count the number of all monic polynomials of degree 2, and subtract the number of these which are reducible.)

6. Show that in $(\mathbb{Z}/p)[x]$, $x^{p^2} - 1$ is the product of all the distinct monic irreducible polynomials of degrees 1 and 2. (Hint: We know by problem 1.4 that each such monic irreducible divides $x^{p^2} - 1$. Use your results in problem 1.5 to find the degree of the product of all these irreducibles.)

7. Use problems 1.3 and 1.6 to show that $x^4 + 1$ is not irreducible in $(\mathbb{Z}/p)[x]$ for all primes $p > 2$, so that by problem 1.2 it is not irreducible in $(\mathbb{Z}/p)[x]$ for any prime $p$. (Hint: $(\mathbb{Z}/p)[x]$ is a U.F.D.).

2. MODULES AND LINEAR TRANSFORMATIONS

8. Let $A$ be the ring $\mathbb{R}[x]$ of polynomials with real coefficients. Define $M$ to be the $A$ module formed by the the complex numbers $\mathbb{C}$ on which $x \in A$ acts by multiplication by $i = \sqrt{-1}$ and elements $r \in \mathbb{R} \subseteq \mathbb{R}[x]$ act by multiplication by $r$. Show that the only $A$-submodules of $M$ are $\{0\}$ and all of $M$. Is this true if instead of letting $x \in A$ by multiplication by $i$ we let $x$ act by multiplication by $-1$?