Intro to modern algebra II

Instructor: Michael Harris

1. Solution to problem set 3

Problem 1. *Part (a): Using polynomial division we get*

$$x^5 + x + 1 = (x^4 + 2x^3 + 4x^2 + 8x + 17)(x - 2) + 35$$

Obviously since $(35, x - 2) = 1$ the polynomials are coprime.

Part (b): Using polynomial division we get

$$x^4 + 2x^3 + 4x^2 + x + 3 = \left(\frac{x^2}{2} + \frac{3x}{4} + \frac{7}{8}\right)(2x^2 + x + 3) + \left(-\frac{17x}{8} + \frac{3}{8}\right)$$

Finally, we observe that $r(x) = -\frac{17x}{8} + \frac{3}{8}$ and $g(x) = 2x^2 + x + 3$ are coprime - either do another polynomial division or observe that $\frac{3}{17}$ is not a root of $g(x)$. Thus the original polynomials are also coprime.

Problem 2. *Note that $R/I = \mathbb{Z}/p^2\mathbb{Z}$, while $R/J = \mathbb{F}_p[X]/X^2 = \{aX + b | a, b \in \mathbb{F}_p\}$.*

Both rings have p^2 elements. They are not isomorphic - for example 1 has additive order p^2 in R/I and p in R/J.

Observe that the nilradical of R/I is the ideal $N_1 = (p)$ and the nilradical of R/J is the ideal $N_2 = (X)$.

Therefore, $(R/I)/N_1 = \mathbb{F}_p = (R/J)/N_2$.

Problem 3. *Recall that an element $a \in \mathbb{Z}/n\mathbb{Z}$ has a multiplicative inverse (i.e. is a unit) if and only if $(a, n) = 1$. Since p is an odd prime the element u should exist. To write it explicitly we could use Euler's theorem (a generalization of Fermat's little theorem)*

$$2^{\varphi(p^2)} \equiv 1 \mod p^2.$$

Since $\varphi(p^2) = p(p - 1)$ we can write $u = 2^{p^2 - p - 1}$.

Let $f(X) = X^2 - (p + 1)$

Observe that $(up + 1)^2 = u^2p^2 + 2up + 1 = p + 1$. Hence $f(X) = (X - (up + 1))(X + (up + 1))$. The roots are $\pm(up + 1)$.

Problem 4. *Exercise 42.*

The fastest way to solve this problem is to use that for any field F, the polynomial ring $F[X]$ is a principal ideal domain. Thus since $(x - a_i)$ are irreducible elements they must divide anything they are not coprime with.

However, it is obvious that $x - a_i$ does not divide $\prod_{j \neq i}(x - a_j)$, since it does not divide any of the terms in the product.

Problem 5. *Exercise 43.*

Let $R = \mathbb{Z}[X]$. The greatest common divisor of X and 2 must be a polynomial of degree 0, i.e. a constant d. Since $h(X) = X$ is a monic polynomial $d = \pm 1$. Thus X and 2 are coprime.

Assume that we could find $f, g \in R$ such that $Xf + 2g = 1$. In order to get a contradiction let us consider the constant term on the left side. Let $g(0) = b$ then $Xf + 2g = 2b + X(\ldots)$. Since $2b = 1$ has no solution in $\mathbb{Z}$ the above equality cannot occur.