Worksheet 21

Math 391, Abstract Algebra

Friday, November 18, 2020

In lecture we found all the irreducible quadratic, cubic, and quartic polynomials in $\mathbb{Z}_2[x]$:

$$x^2 + x + \bar{1}$$

$$x^3 + x + \bar{1} \qquad x^3 + x^2 + \bar{1}$$

$$x^4 + x + \bar{1} \qquad x^4 + x^3 + \bar{1} \qquad x^4 + x^3 + x^2 + x + \bar{1}$$

1. List all the quintic polynomials in $\mathbb{Z}_2[x]$ that have no roots: so the leading term must be x^5, the constant term must be $\bar{1}$ (otherwise $\bar{0}$ would be a root), and there must be an odd number of non-zero terms (otherwise $\bar{1}$ would be a root).

   Hint: There should be $4 + \binom{4}{3} = 8$ of them.

2. If any of these eight quintics are reducible, it must be because they factor as an irreducible quadratic times an irreducible cubic. From the table above we see there are only two ways that can happen. Multiply the irreducible quadratic by each of the irreducible cubics and cross the resulting quintics off your list, leaving a list of the six irreducible quintics in $\mathbb{Z}_2[x]$.

3. Use this calculation to show that $x^5 + 3x^2 + 5$ and $x^5 - 7x^3 + 9$ are irreducible in $\mathbb{Z}[x]$. By Gauss's lemma, which we'll prove next week, this means they're also irreducible in $\mathbb{Q}[x]$.

Challenge: Multiplying polynomials in $\mathbb{Z}_2[x]$ feels a bit like multiplying binary numbers. Is it actually the same?