Selected Solutions for Tutorial 3 – Algebra 2019

Feel free to use whatever resources you have at your disposal.

(1) Familiarize yourself with the Euclidean algorithm and Bezout's lemma. How can it be used to calculate the inverse of an element in $\mathbb{Z}/p\mathbb{Z}$? Work through the full algorithm in some examples of increasing complexity, until you are confident in using it.

(2) If you paid close attention in class, you watched me construct $\mathbb{F}_8$ as the quotient of a polynomial ring. Work through this construction and understand it in detail. Which property of the polynomial used makes this work? Which other polynomial could you have used? Work through both constructions in detail and then seen whether you can find an isomorphism between the two fields you constructed.
Solution: To construct $\mathbb{F}_8$, begin with $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ and form the polynomial ring $\mathbb{F}_2[x]$. Over $\mathbb{F}_2$, there are two irreducible polynomials of degree three, namely

$$x^3 + x + 1 \qquad \text{and} \qquad x^3 + x^2 + 1.$$

In class I constructed $\mathbb{F}_8$ as the quotient

$$\mathbb{F}_2[x]/(x^3 + x + 1).$$

Writing b for the coset of x in this quotient, this gives the identity $b^3 = b+1$. Since the polynomial ring in one variable over a field is a principal ideal domain, and x^3+x+1 is irreducible, the principal ideal $(x^3 + x + 1)$ is prime and hence maximal. It follows that the quotient $\mathbb{F}_2[x]/(x^3 + x + 1)$ is a field.

Alternatively, one could use the ideal (x^3+x^2+1). To be able to tell apart the two constructions, let us write a for the coset of x in this setting. We have constructed two fields with eight elements each.

We now wish to define an isomorphism between these two fields. Since

$$(a + 1)^3 \;=\; a^3 + a^2 + a + 1 \;=\; a,$$

we can use the universal properties of polynomial ring and quotient ring to obtain a well defined $\mathbb{F}_2$-algebra homomorphism f sending b to $a + 1$.

$$x \longmapsto a + 1$$

$$\begin{array}{ccc} \mathbb{F}_2[x] & \longrightarrow & \mathbb{F}_2[x]/(x^3 + x^2 + 1) \\ \downarrow{\scriptstyle q} & \nearrow{\scriptstyle f} & \\ \mathbb{F}_2[x]/(x^3 + x + 1) & & \end{array}$$

An algebra homomorphism is in particular a ring homomorphism, and since source and tartget of f are fields, f is a field homomorphism and therefore injective. Since source and target of f have the same (finite) number of elements, it follows that f is bijective.

(3) If this was easy, construct $\mathbb{F}_{16}$.