Selected Solutions for Tutorial 9 – Algebra 2019

(1) Revisit your construction of $\mathbb{F}_{16}$ and work through it, reframing it as constructing the splitting field of the polynomial $x^{16} - x$ over $\mathbb{F}_2$ step by step.

We had constructed $\mathbb{F}_{16}$ from $\mathbb{F}_4$, so to connect with our original construction, we will construct the splitting field in two steps. One starts by finding the factorization of $x^{16} + x$ into irreducible polynomials. This was tedious, using polynomial division. In Tutorial 10, a more systematic approach was offered, but there is still some ad hoc work involved, so I will record the solution finding process here, rather than a polished solution. Let us pretend that we have not done Tutorial 10 yet, this is Tutorial 9, after all. Start by noticing that 0 and 1 both are roots, so we can divide by $x^2 + x$ to get a degree 14 polynomial

$$x^{16} + x = x(x + 1)(x^{14} + x^{13} + \cdots + 1).$$

We have found the linear factors, what about higher degrees? What even are the irreducible polynomials of degree 2? The list of all polynomials of degree 2 over $\mathbb{F}_2$ is

$$\begin{gathered} x^2 \\ x^2 + 1 \\ x^2 + x \\ x^2 + x + 1. \end{gathered}$$

The first three have roots, so are not irreducible, and at a close look, we recognize the last one to be the one we used when wrting down the multiplication table for $\mathbb{F}_4$ ages ago, although we were not speaking about polynomials yet at the time. O.k., so let's check whether this is a factor (polynomial division again) and indeed,

$$(x^{14} + x^{13} + \cdots + 1) = (x^2 + x + 1)(x^{12} + x^9 + x^6 + x^3 + 1).$$

So,

$$E_1 = \mathbb{F}_2[x]/(x^2 + x + 1)$$

is our first step in constructing the splitting field, and we had once called that coset of x in $a \in E_1$, so let's do that again. Our next step is to find an irreducible polynomial of degree 2 over E_1 and to see whether it is a factor of $x^{12} + x^9 + x^6 + x^3 + 1$. The list of degree 2 polynomials with coefficients in E_1 consists of the polynomials above, which now all have roots in E_1 along with the following list, in which we can find the

irreducible polynomials by elimination.

$$\begin{aligned}
x^2+a &= (x+a+1)^2\\
x^2+a+1 &= (x+a)^2\\
x^2+x+a &\quad \text{irreducible}\\
x^2+x+a+1 &\quad \text{irreducible}\\
x^2+ax &= x(x+a)\\
x^2+ax+1 &\quad \text{irreducible}\\
x^2+ax+a &\quad \text{irreducible}\\
x^2+ax+a+1 &= (x+1)(x+a+1)\\
x^2+(a+1)x &= x(x+a+1)\\
x^2+(a+1)x+1 &\quad \text{irreducible}\\
x^2+(a+1)x+a &= (x+1)(x+a)\\
x^2+(a+1)x+a+1 &\quad \text{irreducible.}
\end{aligned}$$

Now choose any one of the six irreducible options and do polynomial division over E_1 to convince yourself that it is indeed a factor of $x^12+x^9+x^6+x^3+1$. Any choice works, e.g.,

$$E_2 = E_1[x]/(x^2+x+a)$$

or

$$E_2' = E_1[x]/(x^2+x+a+1)$$

so we begin to see that our theorem that any two of these constructions are isomorphic (because they have 16 elements and hence are a splitting field of $x^{16}-x$ over $\mathbb{F}_2$) is quite powerful. If you want to, you can convince yourself that this degree 16 polynomial indeed splits into 16 distinct linear factors over E_2. This is not as hard as it looks, give the coset of x in E_2 a name, say b so that you can name all the elements of E_2, multiply all 16 linear polynomials over E_2 and use the rules $b^2+b=a$ and $a^2+a=1$ to show that this big product is equal to $x^{16}-x$.

Some students went straight from $\mathbb{F}_2$ to $\mathbb{F}_{16}$ by choosing a degree four irreducible polynomial over $\mathbb{F}_2$. How to find such a thing? Still continue using elimination techniques. For a degree four polynomial there are three options: either it is irreducible or it has a root, or it is the product of two irreducible degree 2 polynomials, and if the coefficient field is $\mathbb{F}_2$ there is only one option for that degree 2 polynomial, namely x^2+x+1. So, by elimination, we find that there are three irreducible polynoials of

degree 4 over $\mathbb{F}_2$:

$$\begin{aligned}
x^4 &\quad 0 \text{ is root}\\
x^4+1 &\quad 1 \text{ is root}\\
x^4+x &\quad 0 \text{ is root}\\
x^4+x+1 &\quad \text{ireducible}\\
x^4+x^2 &\quad 0 \text{ is root}\\
x^4+x^2+1 &= (x^2+x+1)^2\\
x^4+x^2+x &\quad 0 \text{ is root}\\
x^4+x^2+x+1 &\quad 1 \text{ is root}\\
x^4+x^3 &\quad 0 \text{ is root}\\
x^4+x^3+1 &\quad \text{irreducible}\\
x^4+x^3+x &\quad 0 \text{ is root}\\
x^4+x^3+x+1 &\quad 1 \text{ is root}\\
x^4+x^3+x^2 &\quad 0 \text{ is root}\\
x^4+x^3+x^2+1 &\quad 1 \text{ is root}\\
x^4+x^3+x^2+x &\quad 0 \text{ is root}\\
x^4+x^3+x^2+x+1 &\quad \text{irreducible.}
\end{aligned}$$

O.k., now we can randomly choose one of these and proceed to build a field extension of degree 4 from it, e.g.,

$$F = \mathbb{F}_2[x]/(x^4+x+1).$$

Indeed, we now have an educated guess for the factorization of $x^{16}+x$ into irreducibles over $\mathbb{F}_2$, namely

$$x^{16}+x = x(x+1)(x^2+x+1)(x^4+x+1)(x^4+x^3+1)(x^4+x^3+x^2+x+1).$$

Note that none of these degree four polynomials remain irreducible over $\mathbb{F}_4 = E_1$:

$$\begin{aligned}
x^4+x+1 &= (x^2+x+a)(x^2+x+a+1)\\
x^4+x^3+1 &= (x^2+(a+1)x+a+1)(x^2+ax+a)\\
x^4+x^3+x^2+x+1 &= (x^2+(a+1)x+1)(x^2+ax+1).
\end{aligned}$$

From this, we can read of the factorization of $x^{16}-x$ into irreducible polynomials over E_1. We don't really need this, but we might as well take notice of it. What is missing is the explicit map from, say, E_1 to F. By trial and error, we find that if c is the coset of x in F, then the element c^2+c is a root of the polynomial x^2+x+1 over F. It follows that we obtain a field homomorphism

$$\begin{aligned}
E_1 &\longrightarrow F\\
a &\longmapsto c^2+c,
\end{aligned}$$

this is the desired inclusion of $\mathbb{F}_4$ in $\mathbb{F}_{16}$.

(2) In the last Tutorial, there was a missing condition: if K is a field and $f : K \to K$ is an automorphism of K *fixing the coefficients* of a given polynomial $p(x) \in K[x]$, then f permutes the roots of p.
(3) Let now K be a field of characteristic p, and let $f : K \to K$ be an automorphism. Recall how $\mathbb{F}_p$ sits inside K as a subfield and prove that f fixes each element of this subfield.