Homework 11

Andrew Tindall
Algebra II

December 6, 2019

Problem 1. Dummit & Foote, 10.5.5: (for an arbitray finite index set): Let

$$\mathfrak{m} = (f_1(x_1), f_2(x_1, x_2), \ldots, f_n(x_1, \ldots x_n))$$

be a maximal ideal in $k[x_1, \ldots x_n]$, where $f_1, \ldots f_n$ are irreducible polynomials such that f_i is irreducible modulo $f_1, \ldots f_{i-1}$. Show that $K = k[x_1, \ldots x_n]/\mathfrak{m}$ is an algebraic field extension of k, so that $k[x_1, \ldots x_n]$ can also be viewed as a subring of $K[x_1, \ldots x_n]$. If $x_1, \ldots x_n$ are mapped to $\alpha_1, \ldots, \alpha_n$ respectively, under the canonical homomorphism $k[x_1, \ldots x_n] \to k[x_1, \ldots x_n]/\mathfrak{m}$, prove that $\mathfrak{m} = k[x_1, \ldots x_n] \cap (x_1 - \alpha_1, \ldots, x_n - \alpha_n) \subset K[x_1, \ldots x_n]$.

This is something of an extension of the weak Nullstellensatz to a not-necessarily algebraically closed field.

Proof. We first show that $K = k[x_1, \ldots x_n]/\mathfrak{m}$ is an algebraic field extension of k. It suffices to show that it is a finite field extension, which it is.

We proceed by induction. First, we know that for $n = 1$, the ring $K_1 = k[x]/(f_1(x))$ is a finite field extension of k: it is a field, because $(f_1(x))$ is maximal, it contains k as a subfield, and it is generated as a k-vector space by the elements $x, x^2, \ldots x^{\deg(f)-1}$.

Now, assume that we know the field $K_{i-1} = k[x_1, \ldots, x_{i-1}]/(f_1(x_1), \ldots f_{i-1}(x_1, \ldots x_{i-1}))$ is a finite field extension of k. We wish to show that $K_i = k[x_1, \ldots x_i]/(f_1, \ldots f_i)$ is a finite field extension of k. Because $(f_1, \ldots f_i)$ is an ideal of $k[x_1, \ldots x_i]$ containing $(f_1, \ldots f_{i-1})$, the third isomorphism theorem for rings gives us

$$\frac{k[x_1, \ldots x_i]}{(f_1, \ldots f_i)} \cong \frac{(k[x_1, \ldots x_i])/(f_1, \ldots f_{i-1})}{(f_1, \ldots f_i)/(f_1, \ldots f_{i-1})}$$

Since x_i does not appear in the polynomials $f_1, \ldots f_{i-1}$, we have the isomorphism

$$k[x_1, \ldots x_i]/(f_1, \ldots f_{i-1}) \cong (k[x_1, \ldots x_{i-1}]/(f_1, \ldots f_{i-1}))[x_i] = K_{i-1}[x_i].$$

Let $\overline{f_i}$ be the image of f_i modulo $f_1, \ldots f_{i-1}$. Using the above isomorphim, we have

$$K_i \cong K_{i-1}[x_i]/(\overline{f_i}(x_1, \ldots x_i)),$$

Where $\overline{f}_i(x_1, \dots x_i)$ is considered as an irreducible polynomial in $K_{i-1}[x_i]$. Using the same argument as in the 1-variable case, K_i is a finite field extension of K_{i-1}, and is therefore a finite field extension of k, of degree $[K_i : k] = [K_i : K_{i-1}] \cdot [K_{i-1} : k]$.

Using the field extension $k \hookrightarrow K$, we can view $k[x_1, \dots x_n]$ as a subring of $K[x_1, \dots x_n]$.

The second half of this problem is unfinished.

□

Problem 2. Dummit & Foote, 10.5.7: Let $(f) = (x^5 + x + 1)$ in Spec$\mathbb{Z}[x]$ viewed as fibered over Spec$\mathbb{Z}$ as in Example 3 following Proposition 55. Prove that there are two closed points in the fiber over (2), three closed points in the fiber over 5, four closed points in the fiber over (19), and five closed points in the fiber over (211).

Proof. The proper method for this solution looks like it involves an interesting application of Galois theory (following chapter 14.8 in Dummit & Foote), but it was a lot simpler to factor these over finite fields using a CAS (Wolfram Alpha).

- (2): Modulo 2, we have

$$\begin{aligned}(x^2 + x + 1)(x^3 + x^2 + 1) &= x^5 + 2x^4 + 2x^3 + 2x^2 + x + 1 \\ &\equiv x^5 + x + 1\end{aligned}$$

  Where x^2+x+1 and x^3+x^2+1 are both irreducible modulo 2, so there are exactly two points in the fiber over (2), corresponding to the ideals $(2, x^2+x+1)$ and $(2, x^3+x^2+1)$.

  Proof that $x^2 + x + 1$ is irreducible modulo 2:

  Because there are only 2 linear polynomials modulo 2, if $x^2 + x + 1$ were reducible, it would have to have either x or $x + 1$ as a factor. Because it has a nonzero constant term, it cannot have x as a factor, so it would have to be equal to $(x + 1)^2$. However, $(x + 1)^2 \equiv x^2 + 1 \not\equiv x^2 + x + 1$. So, this polynomial is not reducible.

  Proof that $x^3 + x^2 + 1$ is irreducible modulo 2:

  If $x^3 + x^2 + 1$ were reducible and had only linear factors, it would again have no factors of x, because it has nonzero constant term. Therefore, it would need to be equal to $(x + 1)^3$. However, $(x + 1)^3 \equiv x^3 + x^2 + x + 1 \not\equiv x^3 + x^2 + 1$.

  This leaves the possibility that $x^3 + x^2 + 1$ is reducible, and has a linear factor and a quadratic irreducible factor. There is only one irreducible quadratic modulo 2, and there is only one possible linear factor, so the only possibility is $(x^2 + x + 1)(x + 1)$. However, $(x^2 + x + 1)(x + 1) \equiv x^3 + 1 \not\equiv x^3 + x^2 + 1$. So, this is an irreducible cubic modulo 2.

- (5): Modulo 5, we have

$$\begin{aligned}(x + 3)(x^2 + x + 1)(x^2 + x + 2) &= (x^3 + 4x^2 + 4x + 3)(x^2 + x + 2) \\ &= x^5 + 5x^4 + 5x^3 + 11x + 6 \\ &\equiv x^5 + x + 1\end{aligned}$$

Where x^2+x+1 and x^2+x+2 are irreducible modulo 5. So, there are 3 points in the fiber over 5, corresponding to $(5, x+3)$, $(5, x^2+x+1)$, and $(5, x^2+x+2)$.

Proof that x^2+x+1 is irreducible modulo 5: if x^2+x+1 had linear factors modulo 5, their constant terms would need to multiply to give 1. The possible pairs are:

- $1, 1$: we have $(x+1)^2 \equiv x^2+2x+1 \not\equiv x^2+x+1$.
- $2, 3$: we have $(x+2)(x+3) \equiv x^2+1 \not\equiv x^2+x+1$.
- $4, 4$: we have $(x+4)(x+4) \equiv x^2+3x+1 \not\equiv x^2+x+1$.

So, x^2+x+1 is irreducible modulo 5.

Proof that x^2+x+2 is irreducible modulo 5: If this polynomial had 2 linear factors modulo 5, their constant terms would need to multiply to give 2. The possible pairs are:

- $1, 2$: we have $(x+1)(x+2) \equiv x^2+3x+2 \not\equiv x^2+x+2$.
- $3, 4$: we have $(x+3)(x+4) \equiv x^2+2x+2 \not\equiv x^2+x+2$.

So, x^2+x+2 is an irreducible quadratic modulo 5.

- (211): Modulo 211, we have

$$\begin{aligned}(x+15)(x+35)(x+51)(x+124)(x+197) &= x^5+422x^4+59924x^3 \\ &\quad +3481078x^2+83710875x+654059700 \\ \\ &= x^5+(2*211)x^4+(284*211)x^3+ \\ &\quad (16598*211)x^2+(396734*211+1)x \\ &\quad +3099809*211+1 \\ \\ &\equiv x^5+x+1\end{aligned}$$

So, there are 5 points in the fiber over (211), corresponding to the 5 linear factors of the polynomial x^5+x+1 modulo 211.

$\square$