Solutions for Tutorial 6 – Algebra 2019

Let $F \subset K$ be fields, and let a be an element of K.

(1) Recall what it means for a to be algebraic over F.

The element a is called algebraic if the F-algebra homomorphism

$$\begin{aligned} \phi : F[x] &\longrightarrow K \\ x &\longmapsto a \end{aligned}$$

has a non-trivial kernel.

(2) In class, you saw a fast forward version of the proof that the field extension generated by F and a is isomorphic to the quotient of a polynomial algebra. In this tutorial, you will fill in the details.

(a) Recall the definition of the relevant map ϕ from a polynomial algebra to K.

The polynomial algebra is $F[x]$. Recall that this polynomial algebra is the free F-algebra on one element: indeed, it is the monomial algebra of free monoid on one element,

$$(\mathbb{N}, +) \cong (\{x^n \mid n \in \mathbb{N}\}, \cdot),$$

where $x^m \cdot x^n = x^{m+n}$. So, there is a unique map of F-algebras ϕ from $F[x]$ to K sending x to a. Explicitly, if

$$p(x) = f_n x^n + f_{n-1} x^{n-1} + \cdots + f_1 x + f_0,$$

then

$$\phi(p) = p(a) = f_n a^n + f_{n-1} a^{n-1} + \cdots + f_1 a + f_0.$$

In other words, ϕ takes a polynomial and evaluates it at a.

(b) Show that $im(\phi)$ is an integral domain.

One checks that $im(\phi) \subseteq K$ is a subring. This holds for any ring homomorphism. Since K is a field, K is an integral domain. Subrings of integral domains are again integral domains, so $im(\phi)$ is an integral domain.

(c) Using the first isomorphism theorem, argue that $ker(\phi)$ is a prime ideal.

The first isomorphism theorem gives an isomorphism

$$F[x]/ker(\phi) \cong im(\phi).$$

So, the quotient on the left is an integral domain. This was our definition of prime ideal.

(d) Show that $F[x]$ is a PID. $F(x)$ is a Euclidean domain, since the degree function a the Euclidean function. The following argument goes through for any Euclidean domain. Let $\mathfrak{a} \subset F[x]$ be a non-zero ideal. Then $\mathfrak{a}$ contains elements of positive degree. Let $a \in \mathfrak{a}$ have minimal degree, i.e.,

$$deg(a) = min\{deg(b) \mid b \in \mathfrak{a} \setminus \{0\}\}.$$

We claim that $(a) = \mathfrak{a}$. To show the inclusion $\subseteq$, note that $a \in \mathfrak{a}$ and that $\mathfrak{a}$ is an ideal. Any element of (a) is of the form $p \cdot a$ with $p \in F[x]$ and hence also contained in $\mathfrak{a}$. To prove the inclusion $\supseteq$, let $b \in \mathfrak{a}$ be given. Then there exists polynomials q and r such that

$$b(x) = a(x) \cdot q(x) + r(x),$$

and $deg(r) < deg(a)$. Since b and a are elements of $\mathfrak{a}$, so is $r = b - q \cdot a$. By the minimality of $deg(a)$, it follows that the remainder r is equal to zero. So, we have $b = q \cdot a \in (a)$.

(e) Prove that $ker(phi)$ is maximal. We saw in class that in a principal ideal domain, prime ideals are maximal.

(f) Prove that $ker(phi) = (p(x))$ where $p(x)$ is an irreducible polynomial.

Since $F[x]$ is a PID, and $ker(\phi)$ is an ideal, since ϕ is a ring homomorphism (prove this), it follows that $ker(\phi) = (p(x))$ for some polynomial $p(x)$. We already saw that $ker(\phi)$ is a prime ideal, so $p(x)$ is a prime element. In class, we saw that in a principal ideal domain, prime elements are irreducible. (In fact, the weaker condition of UFD would have been enough for the last step).

(g) Prove that $im(\phi)$ is a field.

We use the first isomorphism theorem again: since $ker(\phi)$ is a maximal ideal, $F[x]/ker(\phi) \cong im(\phi)$ is a field.

(h) Prove $im(\phi) = F(a)$.

Recall that $F(a)$ was defined to be the smallest subfield field of K containing F and a. To show the inclusion $\subseteq$, let $p(a) = f_n a^n + f_{n-1}a^{n-1} + \cdots + f_1 a + f_0$ be an element in the image of phi. Since the coefficients f_i are elements of F, this expression has to be contained in any field containing F and a. To show the inclusion $\supseteq$, write

$$F(a) = \bigcap_{\substack{F \subseteq E \subseteq K \\ a \in E}} E$$

as the inclusion of all intermediate field extensions containing a and note that $E = im(\phi)$ is such an intermediate extension. Hence $F(a) \subseteq im(\phi)$.

(i) Describe $F(a)$ as a quotient of the polynomial algebra $F[x]$. Putting everything together, we obtain

$$F(a) = im(\phi) \cong F[x]/(p(x),$$

where $p(x)$ is the irreducible polynomial of a.

(3) Work through some examples. A good place to get a feel for what is going on is the extension $\mathbb{F}_2 \subset \mathbb{F}_{16}$.