Lecture Notes, Week 3

Math 480A2: Mathematics of Blockchain Protocols, Fall 2022

Lecturer: Bryan Gillespie

Algebraic Field Extensions

We now turn to the topic of field extensions. In the subsequent discussion we will be interested in the particular type of ring quotient which produces a field, which is characterized by the following.

Definition 1. An ideal I of a commutative ring R is called a **maximal ideal** if I is a proper subset of R, but there is no ideal J satisfying $I \subsetneq J \subsetneq R$.

Proposition 2. *Let R be a commutative ring, and let $I \subseteq R$ be an ideal. Then the quotient ring R/I is a field if and only if I is maximal.*

Proof. Suppose that I is a maximal ideal of R, and suppose that $a + I$ is a nonzero element in R/I. Then $a \notin I$, so the ideal $J = (a) + I$ is strictly larger than I, and since I is maximal, we must have $J = R$.

In particular, $1 \in J$, so we can write $1 = r \cdot a + b$ for some elements $r \in R$ and $b \in I$. Then we have

$$(r + I) \cdot (a + I) = (r \cdot a) + I = (1 - b) + I = 1 + I,$$

so $a + I$ is invertible in R/I, with inverse $r + I$. This implies R/I is a field.

On the other hand, suppose that R/I is a field, and suppose that J is an ideal of R strictly larger than I. If $a \in J \setminus I$, then $a + I$ is a nonzero element of R/I, and so it has an inverse $r + I$ satisfying

$$(r + I) \cdot (a + I) = 1 + I.$$

This means that $1 = r \cdot a + b$ for some element $b \in I$. However, since $I \subseteq J$, the right hand side of the equality is an element of J, so we see that $1 \in J$, and thus $R = (1) \subseteq J$. Since J was an arbitrary ideal larger than I, we conclude that I is maximal. □

We will be particularly interested in extending an existing field with a new element by taking the quotient of a polynomial ring by a maximal ideal. In this setting, the maximal ideals are characterized by the following.

Proposition 3. *Let F be a field, and let $I = (f) \subseteq F[x]$. Then I is a maximal ideal if and only if f is irreducible.*

Proof. If f is a constant polynomial, then both I is not maximal and f is not irreducible, so assume f is non-constant.

Suppose first that I is not maximal. Then there exists an ideal $J = (g)$ with $I \subsetneq J \subsetneq F[x]$. The first inclusion implies that $f = gh$ for some non-invertible polynomial h and $g, h \neq 0$, while the second inclusion implies that g is non-invertible. Since g and h are non-zero and non-invertible, they are non-constant, so $f = gh$ is a representation of f as a product of non-constant polynomials in $F[x]$.

Now suppose that f is not irreducible. Then $f = gh$ for two non-constant polynomials g and h. Suppose that we had $g \in (f)$. Then we could write $g = fh^* = ghh^*$ for some polynomial h^*, which would imply $g(1 - hh^*) = 0$, and thus $hh^* = 1$. This would further imply h is invertible, and therefore is a constant polynomial, a contradiction. Likewise, since g is non-constant, it is not invertible, so there is no polynomial g^* such that $gg^* = 1$, which implies that $1 \notin (g)$. This shows that the ideal $J = (g)$ lies strictly between I and $F[x]$, so I is not maximal. □

Definition 4. Let K be a field and $F \subseteq K$. If F is a field with respect to the arithmetic operations inherited from K, then we say that K is a **field extension** or an **extension field** of F, and write K/F (read as "K over F").

An algebraic structure which will be useful for studying field extensions is that of the *vector space*, defined next. Specifically, it is straightforward to check that when K/F is a field extension, K can naturally be interpreted as a vector space with underlying field F.

Definition 5. A **vector space** over a field F is an additive abelian group V of vectors, along with a scalar multiplication rule $F \times V \to V$ denoted "$\cdot$", satisfying:

- $a \cdot (b \cdot \mathbf{v}) = (ab) \cdot \mathbf{v}$
- $1 \cdot \mathbf{v} = \mathbf{v}$
- $a \cdot (\mathbf{u} + \mathbf{v}) = a \cdot \mathbf{u} + a \cdot \mathbf{v}$
- $(a + b) \cdot \mathbf{v} = a \cdot \mathbf{v} + b \cdot \mathbf{v}$

A set $B \subseteq V$ is called a **basis** of V if every element $v \in V$ can be written uniquely as a finite sum of basis elements multiplied by field elements (a **linear combination**):

$$\mathbf{v} = \sum_{i=1}^{n} a_i \cdot \mathbf{b}_i$$

Every vector space has a basis. Any two bases have the same cardinality, and V is called **finite-dimensional** if this cardinality is finite. In this case, the **dimension** of V is the size of a basis set. An r-dimensional vector space over a field F is *isomorphic* to the vector space F^r of length-r vectors with elements in F and component-wise scalar multiplication, meaning that there is a bijection $V \to F^r$ which preserves vector addition and scalar multiplication.

Remark 6. An equivalent way to define a vector space over a field F is as an abelian group V along with a ring homomorphism $F \to \mathrm{End}(V)$. The abelian group V describes the vectors and their addition operation, and the homomorphism $F \to \mathrm{End}(V)$ describes the scalar multiplication by elements of F.

Definition 7. Let K/F be a field extension, and let $\alpha \in K$. Then α is called **algebraic** over F if it is the root some nonzero polynomial with coefficients in F. Otherwise, it is called **transcendental** over F.

We will primarily be concerned with *algebraic* field extensions, that is, extensions without transcendental elements. The following two important results describe how algebraic elements of a field extension relate to the base field. In general terms: a monic irreducible polynomial may be used to extend a base field with a new algebraic element, an algebraic element of a field extension may be succinctly described by a unique monic irreducible polynomial, and these operations may be suitably interpreted as inverse to each other.

Proposition 8. *Let F be a field, and let f be an irreducible polynomial in $F[x]$. Then:*

- *The ring $K = F[x]/(f)$ is an extension field of F, and the image $\bar{x}$ of x under the quotient map is a root of f in K*
- *The dimension of K as a vector space over F is equal to the degree of f, and the monomials $1, \bar{x}, \bar{x}^2, \ldots, \bar{x}^{\deg f-1}$ give a basis*

Proof. Since f is irreducible over F, (f) is a maximal ideal in $F[x]$, so $K = F[x]/(f)$ is a field. The quotient map $F[x] \to F[x]/(f)$ restricts to a homomorphism $\varphi : F \to F[x]/(f)$ on the subring F, and since f has positive degree, no nonzero element of F maps to 0 in the quotient. Thus the kernel of φ is trivial, and by the first isomorphism theorem, F is isomorphic to its image in K. Evaluating the polynomial f at the image $\bar{x}$ of x in K just gives the additive coset $f + (f)$, which is the zero element. Thus $\bar{x}$ is a root of f in K.

In the following, let $d = \deg f$. We now show that the monomials $1, \bar{x}, \ldots, \bar{x}^{d-1}$ give a vector space basis of K over F. Note first that any additive coset $g + (f)$ may be represented by the polynomial r given by the remainder after division of g by f. In more detail, if $g = qf + r$ for some polynomials q, r with $\deg r < d$, then $g - r = qf \in (f)$, and so $g + (f) = r + (f)$. Because of the degree restriction on r, this gives a representation of $g + (f)$ as a linear combination of the monomials $1, \bar{x}, \ldots \bar{x}^{d-1}$.

Suppose now that a linear relation holds for these monomials, that is, that there are coefficients $a_0, \ldots, a_{d-1} \in F$ such that $\sum_{i=0}^{d-1} a_i \bar{x}^i = 0$. This sum can be represented as the additive coset $p + (f)$, where $p(x) = \sum_{i=0}^{d-1} a_i x^i \in F[x]$, so we have $p + (f) = (f)$. This means that there exists a polynomial q such that $p = qf$. If $q \neq 0$, then qf has degree at least d. However, since p has degree strictly smaller than this, we must have $q = 0$, and thus $p = 0$. This implies that all of the coefficients a_i were themselves zero, so only the trivial linear relation holds between the monomials $1, \bar{x}, \ldots, \bar{x}^{d-1}$, and thus the monomials are linearly independent over F. □

Proposition 9. *Let K/F be a field extension, and let $\alpha \in K$ be an algebraic element. Then there exists a unique monic irreducible polynomial $f \in F[x]$ such that α is a root of f. Additionally:*

- *If g is any polynomial in $F[x]$ that has α as a root, then f divides g*
- *The image $F[\alpha]$ of $F[x]$ under the evaluation map at α is a subfield of K isomorphic to $F[x]/(f)$*

Proof. Let $\varphi : F[x] \to K$ be the evaluation map at α, and let I be the kernel of φ. Since $F[x]$ is a principal ideal domain, $I = (f)$ for some polynomial f, and since α is algebraic, we know that I is nonzero, and thus that f is a non-constant polynomial. By multiplying f by the inverse of its leading coefficient, we may assume without loss of generality that f is monic. By the definition of φ, $f(\alpha) = 0$ in K.

Suppose that f is not irreducible. Then $f = gh$ for some non-constant polynomials $g, h \in F[x]$. But this implies that $f(\alpha) = g(\alpha)h(\alpha) = 0$, so since K is an integral domain, we must have either $g(\alpha) = 0$ or $h(\alpha) = 0$. However, this implies that either g or h must be an element of (f), which is impossible because f is of minimal degree among the non-zero polynomials of (f), and g and h have smaller degree than f. We conclude that f is irreducible.

Suppose now that g is any polynomial in $F[x]$ with $g(\alpha) = 0$. Then g is an element of I, so it can be written as $g = fh$ for some polynomial h (and so f divides g). If h is a constant polynomial, then either $h = 1$, in which case $g = f$, or $h \neq 1$, in which case g is not monic. If h is a non-constant polynomial, then $g = fh$ is a representation of g as a product of non-constant polynomials, so h is not irreducible. Thus f is the unique monic irreducible polynomial in $F[x]$ which has α as a root.

Finally, note that the evaluation map φ at α has image $F[\alpha]$ and kernel (f), so $F[\alpha]$ is a subring of K, and by the first isomorphism theorem, $F[x]/(f) \simeq F[\alpha]$. Since (f) is irreducible, both are fields. □

Definition 10. The unique monic irreducible polynomial described above is called the **irreducible polynomial** for α over F. The degree of this polynomial is called the **degree** of α over F.

Example 11. Let $F = \mathbb{Q}$ and let $f(x) = x^3 - 2$. Then f has no roots over $\mathbb{Q}$, and so has no linear factors, and thus has no irreducible factors of degree 1 or 2. This implies f is itself irreducible over $\mathbb{Q}$. Then $\mathbb{Q}$ can be extended with a new element which is a root of f by taking the quotient $K = \mathbb{Q}[x]/(x^3-2)$. As a vector space, K has dimension 3 over $\mathbb{Q}$, and its elements can be expressed in the form $\{a+bx+cx^2 : a, b, c \in \mathbb{Q}\}$. Sums in this representation work component-wise without issue, and products need to be reduced by using the relation $x^3 - 2 = 0$ to replace any occurrences of x^3 with 2. Noting that x is an element of K whose cube is equal to 2, we can reasonably rename the variable as $\sqrt[3]{2}$. In this case, we get the field

$$\mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} : a, b, c \in \mathbb{Q}\}$$

with addition and multiplication inherited from the corresponding arithmetic in $\mathbb{R}$.

Example 12. Let $F = \mathbb{Q}$ and $K = \mathbb{R}$. Then K is an extension field of F. The number $\alpha = \sqrt{5}$ can be shown to be irrational, but it is a root of the monic irreducible polynomial $f(x) = x^2 - 5$, which is therefore its irreducible polynomial over $\mathbb{Q}$. From this we know that any polynomial with rational coefficients which has $\sqrt{5}$ as a root must have $x^2 - 5$ as a factor. Additionally, we know that $\mathbb{Q}[\sqrt{5}]$ is a field, and can be realized as the quotient $\mathbb{Q}[x]/(x^2-5)$. As a vector space this field can be described as $\mathbb{Q}[\sqrt{5}] = \{a+b\sqrt{5} : a, b \in \mathbb{Q}\}$.

Proposition 13. *Let F be a field, and let $f \in F[x]$ be a polynomial with positive degree. Then there exists a field extension K of F such that f factors into a product of linear factors over K.*

Proof. Suppose f has degree d, and factors as a product of $k \leq d$ irreducible polynomials over F. We use induction on the number $d - k$. If $d - k = 0$, then f can be written as a product of d irreducible factors, meaning that f is already a product of linear terms over F.

Suppose now that $d - k > 0$. Then f has some irreducible factor g of degree at least 2. Letting $F' = F[x]/(g)$, we know that F' is an extension field of F in which g has some root $\alpha \in F'$. Thus over F', the polynomial g factors as $g(x) = (x - \alpha)h(x)$ for a non-constant polynomial $h \in F'[x]$. This means that f has strictly more irreducible factors over F' than it has over F. By induction, there exists a field extension K of F' such that f factors into a product of linear factors over K. Since F' extends F, K is also an extension field of F. $\square$