Module MA3411: Commentary
Field Extensions
Michaelmas Term 2009

D. R. Wilkins

Contents

D Field Extensions

D-1 Vector Spaces

The development of Galois Theory requires some basic linear algebra. But not all that much.

We need to know what a vector space is. We need to know what a basis of a vector space is, and therefore we need to know about linear independence and spanning sets. And we need to know how the dimension of a finite-dimensional vector space is defined.

First let us review the definition of a vector space. A vector space V over a field K is a set that is provided with an operation of addition, defined on V, together with an operation of multiplication, whereby elements of the vector space V may be multiplied by elements of the field K. Elements of the vector field V may be referred to as *vectors*; elements of the field K may be referred to as *scalars*.

A vector space V is required to be an Abelian group with respect to the operation of addition on V. Thus $x+y = y+x$ and $(x+y)+z = x+(y+z)$ for all $x, y, z \in V$. The vector space V has a zero element, which we may denote by 0, or by 0_V, with the property that $x+0 = x$ for all $x \in V$. Also, given any element x of V there exists some element $-x$ of V such that $x + (-x) = 0$. The operation of subtraction on V is defined so that $x - y = x + (-y)$ for all $x, y \in V$.

In addition the vector space is provided with an operation of multiplication-by-scalars whereby a scalar $\lambda \in K$ and a vector $x \in V$ may be multiplied so as to yield a vector λx, where $\lambda x \in V$. Moreover we require that $\lambda(x + y) = \lambda x + \lambda y$, $(\lambda + \mu)x = \lambda x + \mu x$, $(\lambda\mu)x = \lambda(\mu x)$ and $1_K x = x$ for all $\lambda, \mu \in K$ and $x, y \in V$, where 1_K denotes the multiplicative identity element of the field K.

The set $\mathbb{R}^n$ of n-tuples of real numbers is a vector space over the field of real numbers, where the operations of addition and of multiplication-by-scalars are defined in the usual fashion. A vector space over the field of real numbers is often referred to as a *real vector space*. Similarly a vector space over the field of complex numbers is often referred to as a *complex vector space*.

In Galois Theory, and also in Algebraic Number Theory, we deal with vector spaces over the field $\mathbb{Q}$ of rational numbers, and, more generally, with vector spaces over fields K that are themselves finite-dimensional vector spaces over the field $\mathbb{Q}$ of rational numbers.

Let V be a vector space over a field K, and let $x_1, x_2, \ldots, x_k$ be elements of V. These elements $x_1, x_2, \ldots, x_k$ are said to be *linearly dependent* if there

exist elements $\lambda_1, \lambda_2, \ldots, \lambda_k$ of the field K, not all zero, for which

$$\lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_k x_k = 0.$$

These elements $x_1, x_2, \ldots, x_k$ are said to be *linearly independent* if they are not linearly dependent. The elements $x_1, x_2, \ldots, x_k$ are said to *span* the vector space V if, given any element v of V, there exist $\lambda_1, \lambda_2, \ldots, \lambda_k \in K$ such that

$$v = \lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_k x_k.$$

A list $x_1, x_2, \ldots, x_k$ of elements of V is said to constitute a *basis* of V if these elements are linearly independent and also span V. It is easy to verify from these definitions that elements $x_1, x_2, \ldots, x_k$ of the vector space V constitute a basis of V over the field K if and only if, given any element v of V, there exist uniquely determined elements $\lambda_1, \lambda_2, \ldots, \lambda_k$ of K such that

$$v = \lambda_1 x_1 + \lambda_2 x_2 + \cdots + \lambda_k x_k.$$

A vector space is said to be *finite-dimensional* if there exists a finite list of elements of V which is a basis for V over the field K. A fundamental theorem of linear algebra guarantees that the number of elements in any basis of a finite-dimensional vector space is independent of the choice of basis: this number is the *dimension* of the vector space. Thus if a vector space V over a field K is of dimension n for some positive integer n, then every basis of V has n members.

The trivial vector space $\{0\}$ with just one element 0 is considered to be a zero-dimensional vector space.

D-2 The Tower Law

If a field K is a subfield of some field L then L can be regarded as a vector space over the subfield K. We say that L is an *extension field* of K, and we describe the situation where a field K is embedded as a subfield in some field L as a *field extension*, customarily denoted by $L\colon K$. If L is a finite-dimensional vector space over K then this field extension is said to be *finite*. The dimension of this field extension is denoted by $[L\colon K]$.

We must prove that if $M\colon L$ and $L\colon K$ are finite field extensions, then so is $M\colon K$, and that $[M\colon K] = [M\colon L][L\colon K]$. (We must also prove the converse result, but this is straightforward.)

Now L is a finite-dimensional vector space over K, and M is a finite-dimensional vector space over L. Therefore there exists a basis $x_1, x_2, \ldots, x_m$ for L over K, and there exists a basis $y_1, y_2, \ldots, y_n$ for M over L. The essential

idea of the proof is to consider the products $x_i y_j$ of these basis elements, where $1 \leq i \leq m$ and $1 \leq j \leq n$, and to show that the collection of these products constitutes a basis of M as a vector space over K. This requires one to show that these products are linearly independent and that they span M as a vector space over K. These verifications are straightforward exercises in applying the relevant definitions.

D-3 Simple Extensions

Let $L\colon K$ be a field extension, and let $\alpha \in L$. Then $K(\alpha)$ is defined to be the smallest subfield of L containing $K \cup \{\alpha\}$. More specifically, $K(\alpha)$ is the intersection of all subfields of L that are extension fields of K and that also contain α.

Now finite sums and products of elements of a subfield of L belong to that subfield. It follows that $\alpha^j \in K(\alpha)$ for all positive integers j. Therefore

$$c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3 + \cdots + c_n\alpha^n \in K(\alpha).$$

for all positive integers n and for all $c_0, c_1, \ldots, c_n \in K$. But

$$c_0 + c_1\alpha + c_2\alpha^2 + c_3\alpha^3 + \cdots + c_n\alpha^n = f(\alpha),$$

where f is a polynomial $c_0 + c_1x + c_2x^2 + \cdots + c_nx^n$ whose coefficients $c_0, c_1, \ldots, c_n$ belong to the field K. We have thus shown that $f(\alpha) \in K(\alpha)$ for all $f \in K[x]$. Moreover $f(\alpha)^{-1} \in K(\alpha)$ for all $f \in K[x]$ satisfying $f(\alpha) \neq 0$. It follows that $M \subset K(\alpha)$, where

$$M = \{f(\alpha)g(\alpha)^{-1} : f, g \in K[x] \text{ and } g(\alpha) \neq 0\}.$$

Also $K \subset M$, and $\alpha \in M$. We claim that M is itself a subfield of L. Indeed let β and γ be elements of M. Then there exist polynomials f, g, h and k, where $g(\alpha) \neq 0$ and $k(\alpha) \neq 0$, such that $\beta = f(\alpha)g(\alpha)^{-1}$ and $\gamma = h(\alpha)k(\alpha)^{-1}$. Then

$$\begin{aligned} -\beta &= -f(\alpha)g(\alpha)^{-1}, \\ \beta + \gamma &= (f(\alpha)k(\alpha) + h(\alpha)g(\alpha))(g(\alpha)k(\alpha))^{-1}, \\ \beta\gamma &= f(\alpha)h(\alpha)(g(\alpha)k(\alpha))^{-1}, \end{aligned}$$

and therefore $-\beta \in M$, $\beta + \gamma \in M$ and $\beta\gamma \in M$. Moreover if $\beta \neq 0$ then $\beta^{-1} \in M$, because $f(\alpha) \neq 0$ and $\beta^{-1} = g(\alpha)f(\alpha)^{-1}$. This concludes the verification that M is a subfield of L, contained in $K(\alpha)$. Also $K \cup \{\alpha\} \subset M$. But $K(\alpha)$ is by definition the smallest subfield of L containing $K \cup \{\alpha\}$. It

follows that $M = K(\alpha)$. Thus $K(\alpha)$ is the subset of L consisting of all elements of L that can be expressed in the form $f(\alpha)g(\alpha)^{-1}$, where f and g are polynomials with coefficients in K, and where $g(\alpha) \neq 0$.

At this point in the development of the theory of simple extensions we come to a fork in the road. The nature of a simple extension $K(\alpha)\colon K$ depends on whether α is algebraic or transcendental over the ground field K. An element α of an extension field of K is said to be *algebraic* over the field K if it is the root of some non-zero polynomial with coefficients in K. If an element α of an extension field of K is not algebraic over K, then α is said to be *transcendental* over K.

If α is algebraic over K then there exists a unique monic polynomial m_α with coefficients in K with the properties that $m_\alpha(\alpha) = 0$ and every polynomial f with coefficients in K that satisfies $f(\alpha) = 0$ is divisible by the minimum polynomial m_α of α. The simple extension $K(\alpha)\colon K$ is then a finite extension, and its degree is the degree of the minimum polynomial m_α of α. Indeed it can be shown that every element of $K(\alpha)$ can be expressed in the form $f(\alpha)$ for some polynomial f with coefficients in K. Moreover this polynomial f can be chosen so that either $f = 0$ or else $\deg f < \deg m_\alpha$, and moreover the polynomial f satisfying these conditions is uniquely determined. It follows from this that $1_K, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ is a basis for $K(\alpha)$ as a vector space over K, where $n = \deg m_\alpha$, and therefore $[K(\alpha)\colon K] = n = \deg m_\alpha$. (See Theorem 4.5.) We shall discuss simple algebraic extensions in more detail below.

On the other hand, if α is transcendental over K then $K(\alpha)$ is an infinite-dimensional vector space over K. Moreover the subring $K[\alpha]$ of $K(\alpha)$ consisting of those elements of $K(\alpha)$ that are expressible in the form $f(\alpha)$ for some $f \in K[x]$ is an integral domain, and is a proper subring of $K(\alpha)$. Moreover the only elements of $K[\alpha]$ that are invertible in the integral domain $K[\alpha]$ are the elements of the ground field K.

D-4 Simple Algebraic Field Extensions

Let K be a field, let L be an extension field of K, and let α be an element of L. Suppose that α is algebraic over K. Let I denote the set of all polynomials $f(x)$ with coefficients in K which satisfy $f(\alpha) = 0$. Then I is a subset of the polynomial ring $K[x]$.

Now the zero polynomial belongs to I. Let $f, g \in I$. Then $f(\alpha) = 0$ and $g(\alpha) = 0$. But then $-f(\alpha) = 0$ and $f(\alpha)+g(\alpha) = 0$ and therefore $-f \in I$ and $f + g \in I$. Also $h(\alpha)f(\alpha) = 0$ and thus $hf \in I$ for all $h \in K[x]$. Therefore I is an ideal of the polynomial ring. Now, given any ideal of the polynomial ring $K[x]$, there exists some polynomial with coefficients in K that generates

the ideal (see Lemma 3.2). In particular there exists some polynomial $p(x)$ with coefficients in K which generates the ideal I. The ideal I then consists of all polynomial with coefficients in K that are divisible by $p(x)$.

Now let c be a non-zero element of the ground field K. Then $f(x)p(x) = (c^{-1}f(x))(cp(x))$ for all $f \in K[x]$. It follows that a polynomial with coefficients in K is divisible by $p(x)$ if and only if it is divisible by $cp(x)$. Therefore the ideal I is generated by $cp(x)$. Let $m_\alpha(x) = cp(x)$, where is the multiplicative inverse of the leading coefficient of $p(x)$. Then the leading coefficient of $m_\alpha(x)$ is the identity element of K, and thus m_α is a monic polynomial which generates the ideal I. Moreover m_α is the unique monic polynomial generating this ideal I. Indeed let $\overline{m}$ be a monic polynomial that generates I. Then m_α divides $\overline{m}$, and $\overline{m}$ divides m_α, and therefore $\deg m_\alpha \leq \deg \overline{m}$ and $\deg \overline{m} \leq \deg m_\alpha$ and therefore $\deg \overline{m} = \deg m_\alpha$ But m_α divides $\overline{m}$ and thus $\overline{m}(x) = r(x)m_\alpha(x)$ for some polynomial $r(x)$ with coefficients in K. This polynomial r must then be a constant polynomial, and the requirement that both m_α and $\overline{m}$ are monic polynomials then ensures that value of the constant polynomial $r(x)$ is the identity element 1_K of K. Thus $\overline{m} = m_\alpha$.

We have now shown that the element α of the extension field L of K determines a unique monic polynomial $m_\alpha(x)$ with coefficients in K. This polynomial m_α satisfies $m_\alpha(\alpha) = 0$. Moreover if $f(x)$ is a polynomial with coefficients in K, and if $f(\alpha) = 0$, then f is divisible in the polynomial ring $K[x]$ by the polynomial m_α, and thus there exists some polynomial $g(x)$ with coefficients in K such that $f(x) = g(x)m_\alpha(x)$. It follows that $m_\alpha(x)$ is the monic polynomial of smallest degree amongst those polynomials that have α as a root. This polynomial $m_\alpha(x)$ is referred to as the *minimum polynomial* of α. Its basic properties are set out in the statement of Lemma 4.3.

Now suppose that $m_\alpha(x) = g(x)h(x)$, where g and h are polynomials with coefficients in K. Then $0 = m_\alpha(\alpha) = g(\alpha)h(\alpha)$. It follows that either $g(\alpha) = 0$, in which case m_α divides g, or else $h(\alpha) = 0$, in which case m_α divides h. It follows that one of the polynomials $g(x)$ and $h(x)$ must be a constant multiple of $m_\alpha(x)$, and the other must be a constant polynomial. We conclude that the minimum polynomial m_α of α is an irreducible polynomial.

Let

$$K[\alpha] = \{f(\alpha) : f \in K[x]\}.$$

Then $K[\alpha]$ is a subring of the field $K(\alpha)$. It is in fact the subring of $K(\alpha)$ generated by the subset $K \cup \{\alpha\}$. Now any subring of a field is an integral domain, since such a subring is itself a unital commutative ring, and the product of any two non-zero elements of a field is always non-zero. In particular $K[\alpha]$ is an integral domain. We claim that $K[\alpha] = K(\alpha)$, provided that α is algebraic over the ground field K.

Let $f(x)$ be a polynomial with coefficients in K. Suppose that $f(\alpha) \neq 0$. We claim that there exists some polynomial $g(x)$ with coefficients in K such that $f(\alpha)^{-1} = g(\alpha)$. Now the minimum polynomial $m_\alpha(x)$ does not divide $f(x)$. But $m_\alpha(x)$ is an irreducible polynomial. It follows that the only polynomials with coefficients in K that divide both $f(x)$ and $m_\alpha(x)$ are constant polynomials. Thus the polynomials f and m_α are coprime. A basic result concerning coprime polynomials ensures the existence of polynomials g and h with coefficients in K such that $f(x)g(x) + m_\alpha(x)(x) = 1_K$ (see Theorem 3.3). But then $f(\alpha)g(\alpha) = 1_K$, and therefore $f(\alpha)^{-1} = g(\alpha)$. This shows that every non-zero element of the integral domain $K[\alpha]$ is invertible in $K[\alpha]$. It follows that $K[\alpha]$ is itself a field, and therefore $K[\alpha] = K(\alpha)$.

Note that we have shown that if α is algebraic over K then every element of the field $K(\alpha)$ be be expressed as the value $f(\alpha)$ at α of some polynomial f with coefficients in K. This polynomial f may be chosen such that either $f = 0$ or else $\deg f < \deg m_\alpha$. Indeed, given any polynomial $h(x)$ with coefficients in K, there exist polynomials $q(x)$ and $f(x)$ with coefficients in K such that $h(x) = q(x)m_\alpha(x)+f(x)$, where either $f = 0$ or else $\deg f < deg m_\alpha$ (see Lemma 3.1). But then $h(\alpha) = f(\alpha)$, since $m_\alpha(\alpha) = 0$. Now let $\overline{f}$ be a polynomials with coefficients in K for which $\overline{f}(\alpha) = 0$. Suppose that either $\overline{f} = 0$ or else $\deg \overline{f} < \deg m_\alpha$. Then the minimum polynomial m_α divides $f - \overline{f}$. But if $f - \overline{f}$ were a non-zero polynomial then its degree would be less than $\deg m_\alpha$, which is impossible. Therefore $\overline{f} = f$. We have now shown that, given any element z of $K(\alpha)$, there exists a unique polynomial $f(x)$ with coefficients in K such that $f(\alpha) = z$ and either $f = 0$ or else $\deg f < \deg m_\alpha$. It follows that there exist uniquely-determined elements $c_0, c_1, \cdots, c_{n-1}$, where $n = \deg m_\alpha$ such that

$$z = c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_{n-1}\alpha^{n-1}.$$

This shows that $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ is a basis of $K(\alpha)$ as a vector space over the field K. It follows immediately that the simple extension $K(\alpha)\colon K$ is finite, and $[K(\alpha)\colon K] = n = \deg m_\alpha$.

The result we have just obtained is included in the statement of Theorem 4.5. Indeed we have shown that simple algebraic extensions are finite extensions. The converse result follows from Lemma 4.2, which ensures that finite field extensions are algebraic.

D-5 An Alternative Proof regarding Simple Algebraic Field Extensions

Reproduced below is an alternative proof of the results of Lemma 4.4 and Theorem 4.5. This alternative proof depends on the fact that if m is an

irreducible polynomial with coefficients in a field K then the quotient ring $K[x]/(m)$ is a field.

Proof Suppose that the field extension $K(\alpha)\colon K$ is finite. It then follows from Lemma 4.2 that α is algebraic over K.

Conversely suppose that α is algebraic over K. Let $R = \{f(\alpha) : f \in K[x]\}$. Now $f(\alpha) = 0$ if and only if the minimum polynomial m of α over K divides f. It follows that $f(\alpha) = 0$ if and only if $f \in (m)$, where (m) is the ideal of $K[x]$ generated by m. The ring homomorphism from $K[x]$ to R that sends $f \in K[x]$ to $f(\alpha)$ therefore induces an isomorphism between the quotient ring $K[x]/(m)$ and the ring R. But $K[x]/(m)$ is a field, since m is irreducible (Proposition 3.6). Therefore R is a subfield of $K(\alpha)$ containing $K \cup \{\alpha\}$, and hence $R = K(\alpha)$.

Let $z \in K(\alpha)$. Then $z = g(\alpha)$ for some $g \in K[x]$. But then there exist polynomials l and f belonging to $K[x]$ such that $g = lm + f$ and either $f = 0$ or $\deg f < \deg m$ (Lemma 3.1). But then $z = f(\alpha)$ since $m(\alpha) = 0$.

Suppose that $z = h(\alpha)$ for some polynomial $h \in K[x]$, where either $h = 0$ or $\deg h < \deg m$. Then m divides $h - f$, since α is a zero of $h - f$. But if $h - f$ were non-zero then its degree would be less than that of m, and thus $h - f$ would not be divisible by m. We therefore conclude that $h = f$. Thus any element z of $K(\alpha)$ can be expressed in the form $z = f(\alpha)$ for some uniquely determined polynomial $f \in K[x]$ satisfying either $f = 0$ or $\deg f < \deg m$. Thus if $n = \deg m$ then $1, \alpha, \alpha^2 \ldots, \alpha^{n-1}$ is a basis of $K(\alpha)$ over K. It follows that the extension $K(\alpha)\colon K$ is finite and $[K(\alpha)\colon K] = \deg m$, as required. ∎

D-6 Simple Transcendental Field Extensions

Let K be a field, let L be an extension field of K, and let α be an element of L. We say that α is *transcendental* over K if α is not the root of any non-zero polynomial with coefficients in K.

Consider the special case when $K = \mathbb{Q}$ and $L = \mathbb{C}$. We say that a complex number α is *algebraic* if α is the root of some non-zero polynomial with rational coefficients. A complex number α is said to be *transcendental* if it is not algebraic. Thus the *algebraic numbers* are those complex numbers that are algebraic over $\mathbb{Q}$, and the *transcendental numbers* are those complex numbers that are transcendental over $\mathbb{Q}$. Irrational numbers like $\sqrt{2}$ and $\sqrt{3}$ are obviously algebraic over $\mathbb{Q}$. It can be shown that the π and e are transcendental. Now the set $\mathbb{Q}$ of rational numbers is countable. It follows from this that the set of finite lists of rational numbers is countable, and therefore the set of polynomials with rational coefficients is countable. It then follows fairly directly from this that the set of algebraic numbers is

countable. But the set of complex numbers is uncountable. Therefore there must exist uncountably many transcendental numbers.

Now let us return to the general case of simple transcendental field extensions. Let K be a field, and let α an element of some extension field L of K. Suppose that α is transcendental over K. There is a ring homomorphism from the polynomial ring $K[x]$ to the extension field $K(\alpha)$ of K that sends each polynomial f with coefficients in K to its value $f(\alpha)$ at α. Now, because α is transcendental over K, the kernel of this homomorphism is the zero subring of $K[x]$ whose only element is the zero polynomial. Therefore $K[x]$ is isomorphic to a proper subring of $K(\alpha)$. This subring consists of those elements of $K(\alpha)$ that may be expressed in the form $f(\alpha)$ for some $f \in K[x]$; we denote this subring by $K[\alpha]$.

Now the polynomial ring $K[x]$ is an integral domain. Moreover there is a general construction whereby any integral domain R may be embedded in a field Q_R whose elements are represented as fractions r/s, where $r, s \in R$ and $s \neq r$. This field Q_R is referred to as the *field of fractions* associated to the integral domain R. Let r/s and r'/s' be elements of Q_R, where s and s' are non-zero. The definition of Q_R ensures that $r/s = r'/s'$ if and only if $rs' = r's$. Also the operations of addition and multiplication are defined on Q_R so that

$$(r_1/s_1) + (r_2/s_2) = (r_1s_2 + s_1r_2)/(s_1s_2), \quad (r_1/s_1)(r_2/s_2) = (r_1r_2)/(s_1s_2)$$

for all $r_1, r_2, s_1, s_2 \in R$ with $s_1 \neq 0$ and $s_2 \neq 0$. We shall discuss the details of this construction in much more detail below. For now we simply note that the construction just outlined associates to the polynomial ring $K[x]$ a field of fractions $K(x)$ whose elements are represented as ratios $f(x)/g(x)$, where f and g are polynomials with coefficients in K and $g \neq 0$. Such ratios are referred to as *rational functions* over the field K. Rational functions $f(x)/g(x)$ and $h(x)/k(x)$ are considered to be equal to one another if and only if $f(x)k(x) = h(x)g(x)$. The operations of addition and multiplication on the field $K(x)$ are defined so as to correspond to the standard formulae for adding and multiplying fractions. The field $K(x)$ is referred to as the *field of rational functions* over the field K.

Now any injective ring homomorphism $\varphi: R \to L$ from an integral domain R to a field L extends to an injective field homomorphism $\varphi: Q_R \to L$, where Q_R is the field of fractions of the integral domain R. (We shall discuss this also below.) We can apply this result to the homomorphism from the polynomial ring $K[x]$ to the field $K(\alpha)$ that sends $f \in K[x]$ to $f(\alpha)$, where α is an element of some extension field of K that is transcendental over K. This homomorphism is injective and therefore extends to an injective

field homomorphism $\varepsilon_\alpha: K(x) \to K(\alpha)$, where $\varepsilon_\alpha(f/g) = f(\alpha)g(\alpha)^{-1}$ for all polynomials $f, g \in K[x]$ with $g \neq 0$. The image $\varepsilon_\alpha(K(x))$ of this homomorphism is a subfield of $K(\alpha)$ which contains $K \cup \{\alpha\}$. It then follows from the definition of $K(\alpha)$ that $\varepsilon_\alpha(K(x)) = K(\alpha)$. Thus $\varepsilon_\alpha: K(x) \to K(\alpha)$ is an isomorphism of fields.

We conclude from this that if K is a field, if α is an element of some extension field of K, and if α is transcendental over K, then the field $K(\alpha)$ is isomorphic to the field $K(x)$ of rational functions over the field K. The elements of $K(x)$ are represented as fractions $f(x)/g(x)$, where $f(x)$ and $g(x)$ are polynomials with coefficients in K and $g(x) \neq 0$. Moreover elements $f_1(x)/g_1(x)$ and $f_2(x)/g_2(x)$ are equal if and only if $f_1(x)g_2(x) = f_2(x)g_1(x)$, and the isomorphism between $K(x)$ and $K(\alpha)$ sends $f(x)/g(x) \in K(x)$ to $f(\alpha)g(\alpha)^{-1}$.

We now proceed to discuss in detail the construction and basic properties of the field of fractions associated to any integral domain. This discussion should cover the details required to understand the definition and basic properties of the field $K(x)$ of rational functions over some field K.

D-7 The Field of Fractions associated to an Integral Domain

Let R be an integral domain, and let

$$X = \{(r, s) : r, s \in R \text{ and } s \neq 0_R\},$$

where 0_R denotes the zero element of the integral domain R. We define a relation $\sim$ on X, where elements (r, s) and (r', s') of X satisfy $(r, s) \sim (r', s')$ if and only if $rs' = r's$. It is clear that $(r, s) \sim (r, s)$ for all $(r, s) \in X$. Thus the relation $\sim$ on X is reflexive. Also $(r, s) \sim (r', s')$ if and only if $(r', s') \sim (r, s)$. Thus the relation $\sim$ is symmetric.

Let (r, s), (r', s') and (r'', s'') be elements of X, where $r, r', r'', s, s', s'' \in R$, and where s, s' and s'' are non-zero. Suppose that $(r, s) \sim (r', s')$ and $(r', s') \sim (r'', s'')$. Then $rs' = r's$ and $r's'' = r''s'$. It follows that

$$s'(rs'') = (rs')s'' = (r's)s'' = s(r's'') = s(r''s') = s'(sr'').$$

(Note that the above inequalities follow from the requirement that the multiplication operation on the integral domain R be both commutative and associative.) Therefore $s'(rs'' - sr'') = 0$. But $s' \neq 0$, and the product of two non-zero elements of an integral domain must itself be non-zero. It follows that $rs'' - s''r$, and therefore $(r, s) \sim (r'', s'')$. Thus the relation $\sim$ on X

is transitive. We have now shown that $\sim$ is an equivalence relation on the set X.

The equivalence relation $\sim$ on the set X partitions X as a disjoint union of equivalence classes. Let Q_R denote the set consisting of these equivalence classes. Then, given any element (r, s) of the set X, where $r, s \in R$ and s is non-zero, there exists exactly one equivalence class to which (r, s) belongs. Let us denote this equivalence class by r/s. Then

$$Q_R = \{r/s : r, s \in R \text{ and } s \neq 0_R\}.$$

Moreover elements r/s and r'/s' of Q_R satisfy $r/s = r'/s'$ if and only if $rs' = r's$.

We now define operations of addition and multiplication on Q_R. These operations generalize the standard rules for adding and multiplying fractions in elementary arithmetic. Specifically we define

$$(r_1/s_1) + (r_2/s_2) = (r_1s_2 + s_1r_2)/(s_1s_2), \quad (r_1/s_1)(r_2/s_2) = (r_1r_2)/(s_1s_2)$$

for all $r_1/s_1, r_2/s_2 \in Q_R$. However it is necessary to check that these algebraic operations on Q_R are indeed well-defined. This involves showing that the values of $(r_1/s_1) + (r_2/s_2)$ and $(r_1/s_1)(r_2/s_2)$ do not depend on the choice of elements r_1, r_2, s_1, s_2 of the integral domain R to represent the equivalence classes r_1/s_1 and r_2/s_2.

Let $r_1, r_1', r_2, r_2', s_1, s_1', s_2, s_2' \in R$, where s_1, s_1', s_2 and s_2' are non-zero. Suppose that $r_1/s_1 = r_1'/s_1'$ and $r_2/s_2 = r_2'/s_2'$. Then $r_1s_1' = r_1's_1$ and $r_2s_2' = r_2's_2$. We wish to show that

$$(r_1s_2 + s_1r_2)/(s_1s_2) = (r_1's_2' + s_1'r_2')/(s_1's_2').$$

We must therefore show that

$$(r_1s_2 + s_1r_2)(s_1's_2') = (r_1's_2' + s_1'r_2')(s_1s_2).$$

Now

$$\begin{aligned}(r_1s_2 + s_1r_2)(s_1's_2') &= (r_1s_1')(s_2s_2') + (r_2s_2')(s_1s_1') \\ &= (r_1's_1)(s_2s_2') + (r_2's_2)(s_1s_1') \\ &= (r_1's_2' + s_1'r_2')(s_1, s_2),\end{aligned}$$

as required. We have thus verified that the operation of addition on the set Q_R is well-defined. The verification that multiplication on Q_R is well-defined is analogous, but is more straightforward. Now

$$(r_1r_2)(s_1's_2') = (r_1s_1')(r_2s_2') = (r_1's_1)(r_2's_2) = (r_1'r_2')(s_1s_2),$$

and therefore

$$(r_1r_2)/(s_1s_2) = (r_1'r_2')/(s_1's_2').$$

We have now shown that the set Q_R carries well-defined operations of addition and subtraction, defined by the formulae given above.

In fact Q_R, with these operations of addition and multiplication, is a field. An examination of the relevant definitions shows immediately that the operations of addition and multiplication on Q_R are commutative. Let $r_1, r_2, r_3, s_1, s_2, s_3 \in Q_R$, where s_1, s_2 and s_3 are non-zero. Then

$$\begin{aligned}
((r_1/s_1) + (r_2/s_2)) + (r_3/s_3) &= ((r_1s_2 + s_1r_2)/(s_1s_2)) + (r_3/s_3) \\
&= ((r_1s_2 + s_1r_2)s_3 + (s_1s_2)r_3)/((s_1s_2)s_3) \\
&= ((r_1s_2)s_3 + (s_1r_2)s_3 + (s_1s_2)r_3)/((s_1s_2)s_3) \\
&= (r_1(s_2s_3) + s_1(r_2s_3) + s_1(s_2r_3))/(s_1(s_2s_3)) \\
&= (r_1(s_2s_3) + s_1(r_2s_3 + s_2r_3))/(s_1(s_2s_3)) \\
&= (r_1/s_1) + (r_2s_3 + s_2r_3)/(s_2s_3) \\
&= (r_1/s_1) + ((r_2/s_2) + (r_3/s_3)).
\end{aligned}$$

Thus the operation of addition on Q_R is associative. Also

$$\begin{aligned}
((r_1/s_1)(r_2/s_2))(r_3/s_3) &= (r_1r_2/s_1s_2)(r_3/s_3) = ((r_1r_2)r_3)/((s_1s_2)s_3) \\
&= (r_1(r_2r_3))/(s_1(s_2s_3)) = (r_1/s_1)((r_2r_3)/(s_2s_3)) \\
&= (r_1/s_1)((r_2/s_2)(r_3/s_3)).
\end{aligned}$$

Thus the operation of multiplication on Q_R is associative.

Let r, s and t be elements of the ring R, where s and t are non-zero. Then $r(st) = s(rt)$, and therefore $r/s = (rt)/(st) = (r/s)(t/t)$. Also

$$(r/s) + (0_R/t) = (rt + s0_R)(st) = (rt)/(st) = r/s.$$

It follows directly from these identities that $0_R/1_R$ is a zero element for Q_R, and $1_R/1_R$ is a multiplicative identity element for Q_R. Also

$$(r/s) + (-r/s) = (rs + s(-r))/(s^2) = 0_R/s^2 = 0_R/1_R,$$

and thus Q_R is an Abelian group with respect to the operation of addition, and $-(r/s) = (-r)/s$ for all $r/s \in Q_R$. We now note that $r/s = 0_R/1_R$ if and only if $r = r1_R = s0_R = 0_R$. Thus an element r/s of Q_R is non-zero if and only if $r \neq 0_R$ and $s \neq 0_R$. It then follows that every non-zero element of Q_R is invertible. Indeed let r/s be a non-zero element of Q_R. Then $r, s \in R$, $r \neq 0_R$,and $s \neq 0_R$, and $(r/s)^{-1} = s/r$.

Finally we verify that the operations of addition and subtraction on Q_R satisfy the Distributive Law. Let $r_1, r_2, r_3, s_1, s_2, s_3 \in Q_R$, where s_1, s_2 and s_3 are non-zero. Then

$$\begin{aligned}((r_1/s_1) + (r_2/s_2))(r_3/s_3) &= ((r_1s_2 + s_1r_2)/(s_1s_2))(r_3/s_3) \\ &= ((r_1s_2 + s_1r_2)r_3)/((s_1s_2)s_3) \\ &= ((r_1s_2)r_3 + (s_1r_2)r_3)/((s_1s_2)s_3),\end{aligned}$$

and therefore

$$\begin{aligned}&(r_1/s_1)(r_3/s_3) + (r_2/s_2)(r_3/s_3) \\ &\qquad = ((r_1r_3)/(s_1s_3)) + ((r_2r_3)/(s_2s_3)) \\ &\qquad = ((r_1r_3)(s_2s_3) + (s_1s_3)(r_2r_3))/((s_1s_3)(s_2s_3)) \\ &\qquad = ((r_1s_2)(r_3s_3) + (s_1r_2)(r_3s_3))/((s_1s_2)s_3^2) \\ &\qquad = ((r_1s_2)r_3 + (s_1r_2)r_3)/((s_1s_2)s_3) \\ &\qquad = ((r_1/s_1) + (r_2/s_2))(r_3/s_3).\end{aligned}$$

Thus the operations of addition and multiplication on Q_R satisfy the Distributive Law.

We have completed the verification that Q_R, with these operations of addition and multiplication, is a field. This field is referred to as the *field of fractions* associated to the integral domain R.

Now let $\varphi\colon R \to L$ be an injective ring homomorphism from a ring R to a field L. If r, r', s and s' are elements of R, where $s \neq 0$, $s' \neq 0$ and $rs' = r's$, then $\varphi(r)\varphi(s') = \varphi(r')\varphi(s)$, and therefore $\varphi(r)\varphi(s)^{-1} = \varphi(r')\varphi(s')^{-1}$. It follows that there is a well-defined function $\hat{\varphi}\colon Q_R \to L$, where $\hat{\varphi}(r/s) = \varphi(r)\varphi(s)^{-1}$ whenever $r, s \in R$ and $s \neq 0$. Moreover it is straightforward to verify that this function $\hat{\varphi}$ is an injective homomorphism of fields. We conclude from this that every injective ring homomorphism $\varphi\colon R \to L$ from an integral domain R to a field L extends to an injective field homomorphism $\hat{\varphi}\colon Q_R \to L$.