ABSTRACT ALGEBRA II
RINGS AND FIELDS

MARIO L. GUTIERREZ ABED

The Field of Quotients of an Integral Domain

Let D be an integral domain that we wish to enlarge to a field of quotients F[1]. Then we take the Cartesian product

$$D \times D^* = \{(a, b) \mid a, b \in D, b \neq 0\}.$$

Note that $D \times D^*$ still cannot be our desired field F, as it's indicated by the fact that, with $D = \mathbb{Z}$ for instance, different pairs of integers such as $(2, 3)$ and $(4, 6)$ can represent the same rational number. What we need to do then is partition $D \times D^*$ into equivalence classes:

We say that two elements (a, b) and (c, d) in $D \times D^*$ are equivalent (which we denote by $(a, b) \sim (c, d)$) if and only if $ad = bc$.

This relation $\sim$ is in fact an equivalence relation, as can easily be shown. Hence we now define our field F to be the set of all equivalence classes $[(a, b)]$ for $(a, b) \in D \times D^*$, where an element (a_1, b_1) is a representative of the equivalence class $[(a, b)] \iff (a_1, b_1) \sim (a, b)$ (i.e. $\iff a_1 b = b_1 a$).

Now we need to define the binary operations of addition and multiplication on our newly constructed field F:

Lemma. *For $[(a, b)], [(c, d)] \in F$, the equations*

$$[(a, b)] + [(c, d)] = [(ad + bc, bd)] \qquad \textit{and} \qquad [(a, b)][(c, d)] = [(ac, bd)]$$

give well-defined operations of addition and multiplication, respectively, on F.

Remark: Note that with these operations defined on F, the following are true:

- Addition in F is commutative and associative.
- $[(0, 1)]$ is an identity element for addition in F.
- $[(-a, b)]$ is an additive inverse for $[(a, b)]$ in F.
- Multiplication in F is both associative and commutative.
- The distributive laws hold in F.
- $[(1, 1)]$ is a multiplicative identity element in F.
- If $[(a, b)] \in F$ is not the additive identity element, then $a \neq 0$ in D and $[(b, a)]$ is a multiplicative inverse for $[(a, b)]$.

[1] The entire construction can be found on pages 190-194, Fraleigh's. Here I simply state some of the key steps.

Thus we have constructed a field F starting with an integral domain D. Our last step is just to show that F can be regarded as containing D:

Lemma. *The map $i\colon D \longrightarrow F$ given by $i(a) = [(a,1)]$ is an isomorphism from D onto a subring of F.*

Proof. For $a, b \in D$, we have
$$i(a+b) = [(a+b,1)].$$
Also,
$$\begin{aligned} i(a) + i(b) &= [(a,1)] + [(b,1)] \\ &= [(a1+1b,1)] \\ &= [(a+b,1)] \\ \Longrightarrow i(a+b) &= i(a) + i(b). \qquad \text{(Homomorphic property for addition)} \end{aligned}$$

Furthermore, we have that $i(ab) = [(ab,1)]$ and
$$\begin{aligned} i(a)i(b) &= [(a,1)][(b,1)] \\ &= [(ab,1)] \\ \Longrightarrow i(ab) &= i(a)i(b). \qquad \text{(Homomorphic property for multiplication)} \end{aligned}$$

Clearly our map i is surjective, hence we only need to show that it is also injective in order to conclude our proof:
$$\begin{aligned} i(a) &= i(b) \\ \Longrightarrow [(a,1)] &= [(b,1)] \\ \Longrightarrow (a,1) &\sim (b,1) \\ \Longrightarrow a1 &= b1 \\ \Longrightarrow a &= b \qquad \text{(Injectivity checked)} \end{aligned}$$

Thus i is an isomorphism of D with $i[D]$, which is a subdomain of F. □

Remark: Since $[(a,b)] = [(a,1)][(1,b)] = [(a,1)]/[(b,1)] = i(a)/i(b)$ clearly holds in $i[D] \subset F$, and $i[D]$ is isomorphic to D, we have now proven the following theorem:

Theorem. *Any integral domain D can be enlarged to (or embedded in) a field F such that every element of F can be expressed as a quotient of two elements of D. (Such a field F is called a **field of quotients** of D.)*

The next theorem shows that every field containing D contains a subfield which is a field of quotients of D, and that any two fields of quotients of D are isomorphic:

Theorem. *Let F be a field of quotients of D and let L be any field containing D. Then there exists a map $\psi\colon F \longrightarrow L$ that gives an isomorphism of F with a subfield of L such that $\psi(a) = a$ for all $a \in D$.*

Corollary 1. *Every field L containing an integral domain D contains a field of quotients of D.*

Corollary 2. *Any two fields of quotients of an integral domain D are isomorphic.*

Rings of Polynomials

Theorem. *The set $\mathcal{R}[x]$ of all polynomials in an indeterminate x with coefficients in a ring $\mathcal{R}$ is a ring under polynomial addition and multiplication. If $\mathcal{R}$ is commutative, then so is $\mathcal{R}[x]$, and if $\mathcal{R}$ has unity $1 \neq 0$, then 1 is also unity for $\mathcal{R}[x]$.*

Remark: As a result of this theorem, we have that $\mathbb{Z}[x]$ is the ring of polynomials in the indeterminate x with integral coefficients, $\mathbb{Q}[x]$ the ring of polynomials in x with rational coefficients, and so on...

Example: In $\mathbb{Z}_2[x]$, we have

$$(x+1)^2 = (x+1)(x+1) = x^2 + (1+1)x + 1 = x^2 + 1.$$

and

$$(x+1) + (x+1) = (1+1)x + (1+1) = 0x + 0 = 0. \qquad \blacktriangle$$

The following theorem is quite simple and rather obvious but it is extremely important for further studies of field theory:

Theorem (The Evaluation Homomorphisms for Field Theory). *Let F be a subfield of a field E, let α be any element of E, and let x be an indeterminate. The map $\phi_\alpha\colon F[x] \longrightarrow E$ defined by*

$$\phi_\alpha(a_0 + a_1 x + \cdots + a_n x^n) = a_0 + a_1\alpha + \cdots + a_n\alpha^n$$

is a homomorphism of $F[x]$ into E. Also, $\phi_\alpha(x) = \alpha$, and ϕ_α maps F isomorphically by the identity map, i.e. $\phi_\alpha(a) = a$ for $a \in F$. The homomorphism ϕ_α is called the ***evaluation*** *at α.*

Factorization of Polynomials over a Field

Theorem (Division Algorithm for $F[x]$). *Let*

$$f(x) = a_0 + a_1 x + \cdots + a_n x^n \qquad \text{and} \qquad g(x) = b_0 + b_1 x + \cdots + b_m x^m$$

be two elements of $F[x]$, with a_n and b_m both nonzero elements of F and $m > 0$.

Then there are are unique polynomials $q(x), r(x) \in F[x]$ such that $f(x) = g(x)q(x) + r(x)$, with either $r(x) = 0$ or the degree of $r(x)$ is less than the degree m of $g(x)$.

Corollary (**Factor Theorem**). *An element $a \in F$ is a zero of $f(x) \in F[x]$ if and only if $x - a$ is a factor of $f(x)$ in $F[x]$.*

Corollary. *If G is a finite subgroup of the multiplicative group $\langle F^*, \cdot\rangle$ of a field F, then G is cyclic. In particular, the multiplicative group of all nonzero elements of a finite field is cyclic.*

Definition. *A nonconstant polynomial $f(x) \in F[x]$ is **irreducible** over F if $f(x)$ cannot be expressed as a product $g(x)h(x)$ of two polynomials $g(h), h(x) \in F[x]$ both of lower degree than the degree of $f(x)$. Otherwise if this condition is not met we say that $f(x)$ is **reducible** over F.*

Example: Let us show that $f(x) = x^3 + 3x + 2$ in $\mathbb{Z}_5[x]$ is irreducible over $\mathbb{Z}_5$. If $f(x)$ factored into polynomials of lower degree, then there would exist at least one linear factor of the form $x - a$ for some $a \in \mathbb{Z}_5$. But then $f(a)$ would be 0 by the *Factor Theorem.* However

$$f(0) = 2, \quad f(1) = 1, \quad f(-1) = -2, \quad f(2) = 1, \quad \text{and} \quad f(-2) = -2,$$

showing that $f(x)$ has no zeroes in $\mathbb{Z}_5$. Thus $f(x)$ is irreducible over $\mathbb{Z}_5$. ▲

Theorem (**Reducibility of Quadratic and Cubic Polynomials**). *Let $f(x) \in F[x]$, and let $f(x)$ be of degree 2 or 3. Then $f(x)$ is reducible over F if and only if it has a zero in F.*

Proof. ($\Rightarrow$) Let $f(x)$ be reducible over F so that $f(x) = g(x)h(x)$, where both $\deg(g(x))$ and $\deg(h(x))$ are $< \deg(f(x))$. Then, since $f(x)$ is either quadratic or cubic, we must have that either $g(x)$ or $h(x)$ is of degree 1. Now, WLOG, take $\deg(g(x)) = 1$. Then except for a possible factor in F, $g(x)$ is of the form $x - \alpha$. Hence $g(\alpha) = 0$, which in turn implies that $f(\alpha) = 0 \cdot h(x) = 0$, so $f(x)$ has a zero in F.

($\Leftarrow$) This direction is trivial, since by a previous corollary we already know that if $f(\alpha) = 0$ for $\alpha \in F$, then $x - \alpha$ is a factor of $f(x)$, thus $f(x)$ is indeed irreducible over F. □

Theorem 1. *If $f(x) \in \mathbb{Z}[x]$, then $f(x)$ factors into a product of polynomials of lower degrees r and s in $\mathbb{Q}[x]$ if and only if it has such a factorization with polynomials of the same degrees r and s in $\mathbb{Z}[x]$.*

Corollary. *If $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$ is in $\mathbb{Z}[x]$ with $a_0 \neq 0$, and if $f(x)$ has a zero in $\mathbb{Q}$, then it has a zero m in $\mathbb{Z}$, and m must divide a_0.*

Proof. If $f(x)$ has a zero a in $\mathbb{Q}$, then $f(x)$ has a linear factor $x - a$ in $\mathbb{Q}[x]$ by the *Factor Theorem.* But then, by the above theorem, $f(x)$ has a factorization with a linear factor in $\mathbb{Z}[x]$, so for some $m \in \mathbb{Z}$, we must have

$$f(x) = (x - m)\left(x^{n-1} + \cdots - \frac{a_0}{m}\right)$$

Thus a_0/m is in $\mathbb{Z}$, so m divides a_0. □

Example 1: Let us use Theorem 1 to show that

$$f(x) = x^4 - 2x^2 + 8x + 1$$

viewed in $\mathbb{Q}[x]$ is irreducible over $\mathbb{Q}$.

If $f(x)$ has a linear factor in $\mathbb{Q}[x]$, then it has a zero in $\mathbb{Z}$, and by the corollary to Theorem 1, this zero would have to be a divisor in $\mathbb{Z}$ of 1, i.e. ± 1. But $f(1) = 8$ and $f(-1) = -8$, thus such factorization is impossible.

If on the other hand $f(x)$ factors into quadratic factors in $\mathbb{Q}[x]$, then by Theorem 1, it has a factorization

$$(x^2 + ax + b)(x^2 + cx + d)$$

in $\mathbb{Z}[x]$. Equating coefficients of powers of x, we find that we must have

$$bd = 1, \quad ad + bc = 8, \quad ac + b + d = -2, \quad \text{and} \quad a + c = 0$$

for integers $a, b, c, d \in \mathbb{Z}$. From $bd = 1$, we see that either $b = d = 1$ or $b = d = -1$. In any case, $b = d$ and from $ad + bc = 8$, we deduce that $d(a + c) = 8$. But this is impossible since $a + c = 0$. Thus we may conclude that a factorization into quadratic polynomials is also impossible and thus $f(x)$ is irreducible over $\mathbb{Q}$. ▲

Theorem (**Eisenstein Criterion**). *Let $p \in \mathbb{Z}$ be a prime. Suppose that $f(x) = a_0 + \cdots + a_n x^n$ is in $\mathbb{Z}[x]$, and $a_n \not\equiv 0 \mod p$, but $a_i = 0 \mod p$ for all $i < n$, with $a_0 \not\equiv 0 \mod p^2$. Then $f(x)$ is irreducible over $\mathbb{Q}$.*

Example: Take $f(x) = 25x^5 - 9x^4 - 3x^2 - 12$ and notice that for $p = 3$, we have

- $3 \nmid 25$
- $3 \mid -9, -3, -12$
- $3^2 = 9 \nmid -12$.

Hence we have by the *Eisenstein Criterion* that $f(x) = 25x^5 - 9x^4 - 3x^2 - 12$ is irreducible over $\mathbb{Q}$. ▲

Corollary. *The polynomial*

$$\Phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

*is irreducible over $\mathbb{Q}$ for any prime p. This polynomial $\Phi_p(x)$ is known as the p^{th} **cyclotomic polynomial**.*

Theorem. *If F is a field, then every nonconstant polynomial $f(x) \in F[x]$ can be factored in $F[x]$ into a product of irreducible polynomials, the irreducible polynomials being unique expect for order and for unit (that is, nonzero constant) in F.*