2.4 Rings of Fractions

Copyright © 2020, Gregory G. Smith
Last updated: 2020–10–05

The procedure for constructing the rational field $\mathbb{Q}$ from the ring of integers $\mathbb{Z}$ extends easily to any domain R. For ordered pairs (r, s), where $r, s \in R$ and $s \neq 0$, the construction uses the equivalence relation: $(r, s) \equiv (r', s') \Leftrightarrow rs' - r's = 0$. This works only if R is a domain, because this relation is transitive if and only if R has no zerodivisors. Nevertheless, it can be generalized as follows.

2.4.1 Definition. A subset S of a commutative ring R is ***multiplicative*** if every finite product of elements in the set S belongs to S.

This is the same as saying that $1_R \in S$ and the product of two elements of S belongs to S.

2.4.2 Example.

- For any ring element $f \in R$, the set of powers f^n, for all nonnegative integers n, is multiplicative.
- Let P be an ideal in a commutative ring R. For the complement q$R \setminus P$ to be multiplicative, it is necessary and sufficient that P be prime ideal.
- The set of elements of in a commutative ring R that are not zerodivisors is multiplicative.
- For any two multiplicative subsets S and S', the product SS' is also multiplicative.
- The intersection of multiplicative subsets is multiplicative. The intersection of all multiplicative subsets containing a set is the multiplicative set it generates. ◇

The multiplicative set generated by a given subset consists of all the finite products of its elements.

2.4.3 Proposition. *For any subset S in a commutative ring R, there exists a commutative ring $R[S^{-1}]$ and a ring homomorphism $\eta : R \to R[S^{-1}]$ with the following properties:*

- *the elements in the set $\eta(S)$ are units in $R[S^{-1}]$;*
- *for any ring homomorphism $\psi : R \to R'$ such that the elements in the set $\psi(S)$ are units in R', there exists a unique ring homomorphism $\psi' : R[S^{-1}] \to R'$ such that $\psi = \psi' \circ \eta$.*

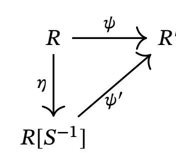

Figure 2.2: Commutative diagram arising from Proposition 2.4.3

Sketch of Proof. We may replace S by the multiplicative subset of R generated by S. Consider the set $R \times S$ with the relation:

$$(r, s) \equiv (r', s') \Leftrightarrow \text{there exists } t \in S \text{ such that } t(rs' - r's) = 0.$$

This relation is clearly reflexive and symmetric. It is also transitive because the equations $t(rs' - r's) = 0$ and $t'(r's'' - r''s') = 0$ yield $tt's'(rs'' - r''s) = t's''\big(t(rs' - r's)\big) + ts\big(t(r's'' - r''s')\big) = 0$ and $tt's' \in S$. Let $R[S^{-1}]$ be the quotient of the set $R \times S$ under the equivalence relation. For any ordered pair (r, s), we write r/s for the equivalent class containing the pair (r, s) in $R[S^{-1}]$ and set $\eta(r) := r/1$.

Two elements in $R[S^{-1}]$ can always be written in the form f/s and g/s with $f, g \in R$ and $s \in S$ with the same denominator. Given f/s and g/s' is $R[S^{-1}]$, we have $f/s = fs'/ss'$ and $g/s' = gs/ss'$.

Consider two ring elements $f = r/s$ and $g = r'/s'$ in $R[S^{-1}]$. The ring elements $(s'r + r's)/ss'$ and $(rr')/(ss')$ depend only on the chosen representatives for f and g. Given another representative $f = r''/s''$, there exists $t \in S$ such that $t(rs'' - r''s) = 0$ whence we obtain $t\big(s's''(s'r+r's)-ss'(s'r''+r's'')\big) = 0$ and $t(s''s'rr'-ss'r''r) = 0$. Hence, the binary operations $(f,g) \mapsto f+g = (s'r+r's)/ss'$ and $(f,g) \mapsto fg = (rr')/(ss')$ are well-defined. One verifies that these operations define a commutative ring structure on $R[S^{-1}]$. The additive identity is $0/1$ and the multiplicative identity is $1/1$. It follows that the map $\eta : R \to R[S^{-1}]$ defined by $\eta(r) = r/1$ is a ring homomorphism. The multiplicative inverse of $s/1$ is $1/s$ in $R[S^{-1}]$.

If the set S contains a nilpotent element then $0 \in S$ and the ring $R[S^{-1}]$ is the zero ring.

Finally, let R' be a commutative ring and let $\psi : R \to R'$ be a ring homomorphism such that the elements $\psi(S)$ are units. There is a map $\psi' : R[S^{-1}] \to R'$ defined by $\psi'(r/s) := \psi(r)\big(\psi(s)\big)^{-1}$. For any $r/s = r''/s''$, there exists $t \in \overline{S}$ such that $t(r''s - rs'') = 0$ whence we have $\psi(t)\big(\psi(r'')\psi(s) - \psi(r)\psi(s'')\big) = 0$. As $\psi(t)$, $\psi(s)$ and $\psi(s'')$ are units, we obtain $\psi(r)\big(\psi(s)\big)^{-1} = \psi(r'')\big(\psi(s'')\big)^{-1}$. One verifies that ψ' is a ring homomorphism. By construction, we have $\psi' \circ \eta = \psi$. Furthermore, the map ψ' is determined by this relation because we have $\psi'(r/s) = \psi'\big((r/1)(1/s)\big) = \psi'(r/1)\,\psi'(1/s) = \psi(r)\,\psi'(1/s)$ and $1 = \psi'(1/1) = \psi'(1/s)\,\psi'(s/1) = \psi'(1/s)\,\psi(s)$. □

The kernel of map $\eta : R \to R[S^{-1}]$ is the set $f \in R$ such that there exists $s \in S$ satisfying $sf = 0$. For the map η to be injective, it is necessary and sufficient that the set S contain no zerodivisor in R.

2.4.4 Remark. For the map η to be bijection, it is necessary and sufficient that every element $s \in S$ be a unit in R. The condition is necessary because $s/1$ is unit in $R[S^{-1}]$. It is sufficient because, for all $t \in S$, the element t is unit in R and $f/t = ft^{-1}/1$ in $R[S^{-1}]$.

2.4.5 Definition. When multiplicative set S consists of the nonzerodivisors in commutative ring R, $R[S^{-1}]$ is the ***total ring of fractions***. When R is a domain, the ring $R[S^{-1}]$ is the ***field of fractions*** of R.

2.4.6 Example. Given a ring element $f \in R$ and $S := \{f^n \mid n \in \mathbb{N}\}$, we have $R_f := R[S^{-1}] \cong R[x]/\langle xf - 1\rangle$. In particular, the Laurent polynomial ring $\mathbb{C}[x, x^{-1}]$ is the ring $\mathbb{C}[x]_x$. ◇

2.4.7 Definition. For any prime ideal P in commutative ring R, we writes R_P for $R[(R \setminus P)^{-1}]$. The elements f/s with $f \in P$ form an ideal P_P in R_P. Every element not in P_P is a unit in R_P. It follows that P_P is the unique maximal ideal in R_P. The process of passing from the ring R to the ring R_P is called ***localization*** at P.

2.4.8 Example. For the prime ideal $P = \langle 0\rangle$ in $\mathbb{Z}$, we have $\mathbb{Z}_{\langle 0\rangle} = \mathbb{Q}$. The ring $\mathbb{C}[x]_{\langle 0\rangle} = \mathbb{C}(x)$ consists of all rational functions. ◇

2.4.9 Example. For any prime number p, the ring $\mathbb{Z}_{\langle p\rangle}$ consists of all rational numbers m/n where the integer n is relative prime to p. ◇

2.5 Univariate Polynomials

Copyright © 2020, Gregory G. Smith
Last updated: 2020–10–06

Polynomials arise in many parts of mathematics. A ***polynomial*** with coefficients in a commutative ring R is a linear combination of power of a variable: $f := a_n\,x^n + a_{n-1}\,x^{n-1} + \cdots + a_1\,x + a_0 = \sum_j a_j\,x^j$, where $a_j \in R$ for all $j \in \mathbb{N}$. The set of all polynomials is denoted by $R[x]$ and the ring operations are defined by

More formally, an infinite sum with finitely many nonzero coefficients.

$$\begin{aligned}\textstyle\sum_j a_j\,x^j + \sum_k b_k\,x^k &= \textstyle\sum_j (a_j + b_j)\,x^j\,,\\ \left(\textstyle\sum_j a_j\,x^j\right)\left(\sum_k b_k\,x^k\right) &= \textstyle\sum_k \left(\sum_j a_j\,b_{k-j}\right) x^k\,.\end{aligned}$$

Iterating this construction yields polynomial rings in more variables: $(R[x])[y] \cong (R[y])[x] \cong R[x,y]$.

The ***monomials*** x^j are independent over R, so $\sum_j a_j\,x^j = \sum_k b_k\,x^k$ if and only if $a_j = b_j$ for all $j \in \mathbb{N}$.

2.5.1 Proposition. *Let $\varphi : R \to R'$ be a ring homomorphism.*

- *The map $\sum_j a_j\,x^k \mapsto \sum_j \varphi(a_j)\,x^j$ defines a ring homomorphism from $R[x]$ to $R'[x]$.*
- *For any ring element $a \in R'$, there is a unique ring homomorphism $\widetilde{\varphi} : R[x] \to R'$ that agrees with the map φ on constant polynomials*

Comment on the Proof. The map $\widetilde{\varphi}$ is a composition of the first ring homomorphism and the evaluation map $\mathrm{ev}_a : R'[x] \to R'$ defined by $\mathrm{ev}_a(f) := f(a)$. □

2.5.2 Definition. For any nonzero polynomial $f \in R[x]$, the ***degree*** $\deg(f)$ is the largest integer k such that the coefficient a_k of the monomial x^k is nonzero. The nonzero element $a_m \in R$ satisfying $m = \deg(f)$ is the ***leading coefficient*** of the polynomial. A ***monic*** polynomial is one whose leading coefficient is 1_R.

2.5.3 Lemma. *Let f and g be two nonzero polynomials in $R[x]$.*

- *If $\deg(f) \neq \deg(g)$, then the sum $f + g$ is nonzero and its degree is $\deg(f+g) = \max(\deg(f), \deg(g))$. If $\deg(f) = deg(g)$, then the degree of the sum satisfies $\deg(f+g) \leqslant \deg(f)$.*
- *We have $\deg(f\,g) \leqslant \deg(f) + \deg(g)$ and equality holds if the leading coefficient of f or g is a nonzerodivisor in R.*

Proof. Let a_m be the leading coefficient of f and let b_n be the leading coefficient of g. It follows that the leading coefficient the sum $f+g$ is a_m when $m > n$ and b_n with $m < n$. When $m = n$, the coefficient of x^m in the sum $f + g$ is $a_m + b_n$ and the coefficients of all monomials of higher-degree are zero, so $\deg(f+g) \leqslant m$. The coefficient of x^{m+n} in the product $f\,g$ is $a_m\,b_n$ and the coefficients of all monomials of higher-degree are zero, so $\deg(f\,g) \leqslant \deg(f) + \deg(g)$. □

2.5.4 Proposition. *For any domain R, the polynomial ring $R[x]$ is also a domain and the units in $R[x]$ are the units in R.*

Proof. Suppose that f and g are nonzero polynomials in $R[x]$. Since $\deg(fg) = \deg(f) + \deg(g) \geqslant 0$, it follows that $fg \neq 0$. If $fg = 1$, then we have $\deg(f) + \deg(g) = \deg(1) = 0$. Hence, f and g are both polynomials of degree 0 and therefore elements of R. □

2.5.5 Theorem (Euclidean Division). *Let f and g be nonzero elements in $R[x]$ of degrees m and n respectively. Denote the leading coefficient of f by a_m and set $k := \max(n - m + 1, 0)$. There exists $q, r \in R[x]$ such that $a_m^k\, g = q\, f + r$ where $\deg(r) < m$. When a_m is a nonzerodivisor in R, the polynomials q and r are uniquely determined by these properties.*

Proof. When $n < m$, take $q = 0$ and $r = g$. When $n \geqslant m$, we proceed by induction on n. Set $f := \sum_{j=0}^{m} a_j\, x^j$ and write b_n for the leading coefficient of g. It follows that $\deg(a_m^k\, g - a_m^{k-1}\, b_n\, x^{n-m} f) < n$. The induction hypothesis implies that, there exists $p, r \in R[x]$ such that $a_m^{k-1}(a_m\, g - b_n x^{n-m} f) = p\, f + r$ where $\deg(r) < m$. Hence, we obtain $a_m^k\, g = (a_m^{k-1}\, b_n x^{n-m} + p) f + r$ and $q := a_m^{k-1}\, b_n x^{n-m} + p$.

Consider $q, q', r, r' \in R[x]$ such that $a_m^k\, g = qf + r = q'f + r'$ where $\deg(r) < m$ and $\deg(r') < m$. It follows that $(q - q')f = (r' - r)$ and $\deg(r' - r) < m$. Since $m + \deg(q - q') = \deg(r' - r) < m$, we conclude that $q = q'$ and $r = r'$. □

2.5.6 Definition. A ***root*** of polynomial f in $R[x]$ is a ring element $a \in R$ such that $\mathrm{ev}_a(f) = f(a) = 0$.

2.5.7 Corollary. *For any polynomial $f \in R[x]$, there exists $q \in R[x]$ such that $f(x) = q(x)\,(x - a)$ if and only if we have $f(a) = 0$.*

Proof. Euclidean division implies that there exists q and r in $R[x]$ such that $f(x) = q(x)\,(x - a) + r(x)$ where $\deg(r) < 1$. Hence, we have $r(x) \in R$. Evaluating at a yields $f(a) = q(a)(0) + r$, so we obtain $f(x) = q(x)(x - a) + f(a)$. □

2.5.8 Proposition. *Let f be a polynomial in $R[x]$ and let $a \in R$ in a ring element. For any nonnegative integer $m \in \mathbb{N}$, the following are equivalent:*
(a) *the polynomial f is divisible by $(x - a)^m$ by not by $(x - a)^{m+1}$;*
(b) *there exists $g \in R[x]$ such that $f(x) = (x - a)^m\, g(x)$ and $g(a) \neq 0$.*
Moreover, whenever $f \neq 0$, there exists a unique nonnegative integer m satisfying these conditions.

Proof.
(a) ⇒ (b): Follows from Corollary 2.5.7.
(b) ⇒ (a): If $f(x) = (x - a)^m\, g(x)$ where g does not have a as root, then f is divisible by $(x - a)^m$. Suppose that $h \in R[x]$ exists such that $f(x) = (x - a)^{m+1}\, h(x)$. Since $(x - a)^m$ is not a zerodivisor in $R[x]$, we would have $g(x) = (x - a)\, h(x)$ which implies that $g(a) = 0$ which is contradiction. □