2.10 Noetherian Rings

2.10.1 Definition. A ring R is ***noetherian*** if every ascending chain of ideals in R is eventually constant. More explicitly, for any increasing sequence of ideals

$$I_0 \subseteq I_1 \subseteq \cdots \subseteq I_{k-1} \subseteq I_k \subseteq I_{k+1} \subseteq \cdots ,$$

there exists a nonnegative integer m such that $I_m = I_{m+1} = \cdots$.

2.10.2 Example. Having only two ideals, any field is noetherian. ✧

2.10.3 Example. The polynomial ring $\mathbb{Q}[x_0, x_1, x_2, \dots]$ with infinitely many variables is non-noetherian because there exists an increasing sequence of distinct ideals $\langle x_0 \rangle \subset \langle x_0, x_1 \rangle \subset \langle x_0, x_1, x_2 \rangle \subset \cdots$. ✧

2.10.4 Lemma. *Let R be ring. For any ascending chain $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$ of ideals in R, the union $I = \bigcup_{j=0}^{\infty} I_j$ is an ideal in R. Moreover, when I is finitely generated, there exists a nonnegative integer m such that $I = I_m$.*

Proof. Let $f, g \in I$ and $r \in R$. Hence, there exists nonnegative integers i and j such that $f \in I_i$ and $g \in I_j$. Without loss of generality, we may assume $j \geqslant i$. Since $I_i \subseteq I_j$, we have $f \in I_j$. Since I_j is an ideal, it follows that $rf + g \in I_j \subseteq I$, so I is an ideal.

Suppose that $I = \langle f_1, f_2, \dots, f_n \rangle$. For each $1 \leqslant i \leqslant n$, there exists a nonnegative integer $\ell(i)$ such that $f_i \in I_{\ell(i)}$. Setting

$$m := \max\{\ell(1), \ell(2), \cdots, \ell(n)\},$$

we have $f_i \in I_m$ for all $1 \leqslant i \leqslant n$. Therefore, we conclude that $I = \langle f_1, f_2, \dots, f_n \rangle \subseteq I_m \subseteq I$, so $I = I_m$. □

2.10.5 Theorem. *A commutative ring R is noetherian if and only if every ideal in R is finitely generated.*

Proof.

(⇒) Suppose that R is noetherian and let I be an ideal in R. If $I = \langle 0 \rangle$, then it is certainly finitely generated. Otherwise, pick a nonzero ring element $f_0 \in I$. If $I = \langle f_0 \rangle$, then again I is finitely generated. Otherwise, pick a ring element $f_1 \in I \setminus \langle f_0 \rangle$. Again, if $I = \langle f_0, f_1 \rangle$ then I is finitely generated. Otherwise, continue this process. If one does not produce a finite set of generators of I, then we would have the ascending chain $\langle f_0 \rangle \subset \langle f_0, f_1 \rangle \subset \langle f_0, f_1, f_2 \rangle \subset \cdots$ of ideal, contradicting noetherian condition.

(⇐) Suppose that every ideal in R is finitely generated. Consider an ascending chain $I_0 \subseteq I_1 \subseteq I_2 \subseteq \cdots$ of ideals in the ring R and the union $I := \bigcup_{j=0}^{\infty} I_j$. Lemma 2.10.4 shows that I is ideal. Every ideal in R is finitely generated, so Lemma 2.10.4 also shows that there is a nonnegative integer m such that $I = I_m = I_{m+1} = \cdots$. □

For any field K, the rings $\mathbb{Z}$, $K[x]$, and $K[[x]]$ are noetherian.

2.10.6 Corollary. *Every principal ideal domain is noetherian.* □

2.10.7 Proposition. *Every principal ideal domain is a unique factorization domain.*

Proof. Combining Proposition 2.9.6 and Proposition 2.9.8, it enough to prove that every nonzero nonunit in a principal ideal domain is a product of irreducibles.

Suppose that the ring R is principal ideal domain and the nonzero nonunit $f \in R$ is not a product of irreducibles. Since ring element f is not irreducible, it follows that $f = gh$ where neither g and h are units. If both g and h were a product of irreducibles, then so would f. Hence, at least one factor, say g, is not irreducible. We have $\langle f \rangle \subset \langle g \rangle$. Repeating this process, we produce an ascending chain of ideals that is not eventually constant. However, Corollary 2.10.6 shows that R is noetherian which is a contradiction. □

2.10.8 Corollary (Fundamental theorem of arithmetic). *Any nonzero integer m can be written as $m = u\,p_1\,p_2\,\cdots\,p_\ell$ where $u = \pm 1$, each p_j is prime integer, and $\ell \geqslant 0$. This expression is unique except for the ordering of the primes.* □

2.10.9 Theorem (Hilbert Basis). *For any noetherian commutative ring R, the polynomial ring $R[x]$ is also noetherian.*

Proof. Let J be and ideal in $R[x]$. We claim that J is finitely generated. For all nonnegative integers n, let I_n denote the set of all leading coefficients of polynomials of degree n in J. Since addition and multiplication by elements in R is defined coefficientwise in R, we see that I_n is an ideal in R. We have $I_n \subseteq I_{n+1}$ because $f = a\,x^n + \cdots \in I_n$ implies that $xf = a\,x^{n+1} + \cdots \in I_{n+1}$. Since R is noetherian, there exists a nonnegative integer such that $I_m = I_{m+1} = \cdots$ and, for all $0 \leqslant i \leqslant m$, each $I_n = \langle a_{i,1}, a_{i,2}, \ldots, a_{i,k_i} \rangle$ for some nonnegative integer k_i. Choose elements $f_{i,j} \in J$ such that the leading coefficient of $f_{i,j} = a_{i,j}$ for all $0 \leqslant i \leqslant$ and $1 \leqslant j \leqslant k_i$. We claim that the ideal J is generated these polynomials.

Suppose there is a polynomial $g \in J$ of minimal degree n such that $g \notin J' := \langle f_{i,j} \mid 0 \leqslant i \leqslant m \text{ and } 1 \leqslant j \leqslant k_i \rangle$. Set $\ell := \min(m, n)$. The definition of the ideal I_ℓ implies that the leading coefficient of g has the form $r_1\,a_{\ell,1} + r_2\,a_{\ell,2} + \cdots + r_{k_\ell}\,a_{\ell,k_\ell}$ for some $r_1, r_2, \ldots, r_{k_\ell} \in R$. It follows that $h := g - x^{n-\ell}(r_1\,f_{\ell,1} + r_2\,f_{\ell,2} + \cdots + r_{k_\ell}\,f_{\ell,k_\ell})$ has degree less that n. Our choose of g guarantees that $h \in J'$. However, this implies that $g = h + x^{n-\ell}(r_1\,f_{\ell,1} + r_2\,f_{\ell,2} + \cdots + r_{k_\ell}\,f_{\ell,k_\ell})$ belongs to J', which contradicts our supposition. □

2.10.10 Corollary. *For any nonnegative integer n and any noetherian ring R, the polynomial ring $R[x_1, x_2, \ldots, x_n]$ is also noetherian.* □

2.11 Factoring polynomials

Last updated: 2020–10–22

To define the content, we need to know that greatest common divisors exist. The greatest common divisor, if it exists, is unique only up to multiplication by a unit. Hence, the content of a polynomial is an equivalence class.

2.11.1 Definition. Let R be a unique factorization domain and let $f := a_m x^m + a_{m-1} x^{m-1} + \cdots + a_1 x + a_0 \in R[x]$. The ***content*** of f is defined to be $\operatorname{cont}(f) := \gcd(a_m, a_{m-1}, \ldots, a_0)$. The polynomial f is ***primitive*** if $\operatorname{cont}(f) = 1$.

2.11.2 Lemma (Gauss). *Let R be a unique factorization domain. For any two polynomials $f, g \in R[x]$, we have $\operatorname{cont}(fg) = \operatorname{cont}(f)\operatorname{cont}(g)$. In particular, if f and g are primitive, then the product $f\,g$ also is.*

Proof. Write $f = \operatorname{cont}(f)\, f^\circ$ and $g = \operatorname{cont}(g)\, g^\circ$ where f°, g° are primitive. Since we have $f\,g = \operatorname{cont}(f)\operatorname{cont}(g)\, f^\circ g^\circ$, it suffices to verify that $f^\circ g^\circ$ is primitive. Let $f^\circ = a_0 + a_1 x + \cdots + a_m x^m$ and $g^\circ = b_0 + b_1 x + \cdots b_n x^n$. Suppose that the coefficients of $f^\circ g^\circ$ have a common divisor d which is not a unit. If p is a prime divisor of d, then p must divide all the coefficients of $f^\circ g^\circ$. Since f° and g° are primitive, p does not divide all the coefficients of f° or g°. Let a_r be the first coefficient of f° not divisible by p and let b_s be the first coefficient of g° not divisible by p. Consider the coefficient of x^{r+s} in $f^\circ g^\circ$; it has the form

$$a_r\, b_s + (a_{r+1}\, b_{s-1} + a_{r+2}\, b_{s-2} + \cdots) + (a_{r-1}\, b_{s+1} + a_{r-2}\, b_{s+2} + \cdots)\,.$$

By hypothesis p divides this sum. Moreover, all the terms in the first parenthesis are divisible by p (because p divides b_j for all $j < s$) and all terms in the second parenthesis are divisible by p (because p divides a_i for all $i < r$). It follows that p divides $a_r\, b_s$. As p is prime, p divides either a_r or b_s contrary to our choice of a_r and b_s. This contradiction shows that no prime divides all the coefficients of $f^\circ g^\circ$ and hence $f^\circ g^\circ$ is primitive. □

2.11.3 Lemma. *Let R be a unique factorization domain and let K be its field of fractions.*

- *For any nonzero polynomial $f \in K[x]$, we have $f = c\, f^\circ$ where $c \in K$ and f° is a primitive polynomial in $R[x]$. This factorization is unique up to multiplication by a unit of R.*
- *Let $f \in R[x]$ be a polynomial having positive degree. If f is irreducible in $R[x]$, then f is irreducible in $K[x]$.*

Proof.

- Finding a common denominator d for the nonzero coefficients of f, we obtain $f = (1/d)\,\tilde{f}$ where $\tilde{f} \in R[x]$. Setting $c := \operatorname{cont}(\tilde{f})/d$, it follows that $f = c\, f^\circ$ where $f^\circ \in R[x]$ is primitive. Suppose that $f = a/b\, g$ where $a/b \in K$ and $g \in R[x]$ is primitive. It follows that $a\, d\, g = b\, \operatorname{cont}(f)\, f^\circ$. Taking the content of both sides yields $u\, a\, d = b\, \operatorname{cont}(f)$ for some unit $u \in R$. We deduce that $u\, g = f^\circ$.

- Since $\mathrm{cont}(f)$ divides f, the polynomial f is primitive in $R[x]$. Suppose that f is reducible in $K[x]$. It follows that $f = g_1 g_2$ where $g_j \in K[x]$ and $\deg(g_j) > 0$ for all $1 \leqslant j \leqslant 2$. The first part implies $g_j = c_j h_j$ where $c_j \in K$ and $h_j \in R[x]$ is primitive. Hence, $f = c_1 c_2 h_1 h_2$ and the product $h_1 h_2$ is primitive by Lemma 2.11.2. The first part implies f and $h_1 h_2$ differ by multiplication by a unit of R, which contradicts the irreducibility of $f \in R[x]$. □

2.11.4 Theorem. *For any unique factorization domain R, the polynomial ring $R[x]$ is also a unique factorization domain.*

Proof. Let K be the field of fractions for R. Consider a nonzero polynomial $f \in R[x]$. Since $K[x]$ is a unique factorization domain, we can write $f = p_1 p_2 \cdots p_r$ where $p_j \in K[x]$ is irreducible for all $1 \leqslant i \leqslant r$. Lemma 2.11.3 implies that $p_j = c_j q_j$ where $c_j \in K$ and $q_j \in R[x]$ is primitive. Hence, we see that $f = c\, q_1 q_2 \cdots q_r$ where $c = \prod_j c_j \in K$. Write $c = a/b$ where $a, b \in R$. Taking contents, we obtain $\mathrm{cont}(b f) = \mathrm{cont}(a\, q_1 q_2 \cdots q_r) = a$ by Lemma 2.11.2. Thus, we obtain $b\ \mathrm{cont}(f) = a$ so b divides a and $\mathrm{cont}(f) = c \in R$. Since each q_j is irreducible in $K[x]$, it is irreducible in $R[x]$. The ring R is a unique factorization domain, so we have $c = u\, d_1 d_2 \cdots d_s$ where each d_i is irreducible in R and $u \in R$ is a unit. It follows that $f = u\, d_1 d_2 \cdots d_s\, q_1 q_2 \cdots q_r$ is a factorization of f into a product of irreducible elements in $R[x]$.

It remains to check uniqueness. Suppose that we have a second factorization: $f = u'\, d_1' d_2' \cdots d_t' q_1' q_2' \cdots q_k'$ where each $q_j' \in R[x]$ is primitive and $d_j' \in R$ is irreducible. Since this is also a factorization in $K[x]$ and the factorization there is unique, it follows that $r = k$ and $q_j' = q_j$ (up to units and reordering). If primitive polynomials differ by a unit in $K[x]$, then they also differ by a unit in $R[x]$. Furthermore, we have $\mathrm{cont}(f) = u'\, d_1' d_2' \cdots d_t' = u\, d_1 d_2 \cdots d_s$ so $s = t$ and $d_j' = d_j$ (up to units and reordering). □

2.11.5 Corollary. *For any nonnegative integer n and any unique factorization domain R, the polynomial ring $R[x_1, x_2, \ldots, x_n]$ is also a unique factorization domain.* □