NUMBER THEORY

github.com/danimalabares/stack

Contents

1. Rings

Definition 1.1. A ring R is called a *domain* if it has no proper zero divisors, that is, if $ab = 0$ then $a = 0$ or $b = 0$.

2. Polynomial rings

Lemma 2.1. *The ring of polynomials in one indeterminante over a domain R is a domain.*

Proof. Suppose that $fg = 0$ for $f, g \in R[x]$. Then the leading coefficient of fg is $a_n b_m$ where $f = \sum_{i=1}^n a_i x^i$ and $g = \sum_{i=1}^m b_i x^i$. Since $a_n b_m = 0$, then $a_n = 0$ or $b_m = 0$, but this is a contradiction since R is a domain and $a_n \neq 0$, $b_m \neq 0$. □

3. Greatest common divisor and least common multiple

Following is the universal definition of lcm and gdc:

Definition 3.1. A *least common multiple* of $a, b \in R$ is an element d such that if for every $c \in R$, if $a, b | c$ then $d | c$.

A *greatest common divisor* of $a, b \in R$ is an element d such that for every $c \in R$, if $c | a, b$ then $c | d$.

But it looks like it shall be easier to define them as follows:

Definition 3.2. A *least common multiple* of $f, g \in R[x]$ is the monic polynomial d of smallest degree such that $f, g | d$.

A *greatest common divisor* of $f, g \in R[x]$ is the monic polynomial d of greatest degree such that $d | f, g$.

Lemma 3.3. *If R is a UFD, in $R[x]$ there exist lcm and mcd, and are unique up to multiplication by units.*

Proof. We can order by degree, and those of the same degree order by the leading term… but this requires an order in R. □

4. Euclidean domains

Definition 4.1. A domain R is an *Euclidean domain* if there is a function $\varphi : R \to \mathbb{Z}_+$, the positive integers, such that

(1) $\varphi(ab) \geq \varphi(a)$ for all $a, b \in R$,
(2) For all $a, b \in R$ with $\varphi(a) \geq \varphi(b)$, there are $q, r \in R$ such that

$$a = bq + r \qquad \text{and} \qquad \varphi(r) < \varphi(b).$$

Remark 4.2. Item 1 is equivalent to asking that if a divides b then $\varphi(a) \leq \varphi(b)$.

Theorem 4.3 (Euclidean algorithm for polynomial rings)**.** *Let R be a domain and $f, g \in R[x]$ with the leading coefficient of g a unit and deg$(f) \geq$ deg(g). Then there are polynomials $q, r \in R[x]$ such that $f = qg + r$ with deg$(r) <$ deg$g$.*

Proof. Since deg(r) must be smaller than deg$q$ and the leading coefficient of a product is the product of the leading coefficients of the factors, we readily see that the leading coefficient of q must be $L(f)/L(g)$ and of degree $n - m$, where L is the leading coefficient function and deg$(f) = n$, deg$(g) = m$.

We are lead to the following natural strategy: write $g = L(g)x^m + g_1$ for some g_1 of degree strictly smaller than m. Likewise, write $f = L(f)x^n + f_1$.

Then multiply g with the leading term of q to obtain

$$\begin{aligned} g\left(\frac{L(f)}{L(g)}x^{n-m}\right) &= (L(g)x^m + g_1)\left(\frac{L(f)}{L(g)}x^{n-m}\right) \\ &= L(f)x^n + g_1\left(\frac{L(f)}{L(g)}x^{n-m}\right). \end{aligned}$$

Add f_1 on both sides to obtain f:

$$\begin{aligned} g\left(\frac{L(f)}{L(g)}x^{n-m}\right) + f_1 &= L(f)x^n + f_1 + g_1\left(\frac{L(f)}{L(g)}x^{n-m}\right) \\ \iff f &= g\left(\frac{L(f)}{L(g)}x^{n-m}\right) + f_1 - g_1\left(\frac{L(f)}{L(g)}x^{n-m}\right) \end{aligned}$$

We have great candidates for q and r, except that put this way it is not necessarily true that the remainder will have degree strictly smaller than g. However, it is true that it will have degree strictly smaller than the degree of f. Then we can just repeat the process until we arrive at a reminder with degree strictly smaller than the degree of g. □

5. Unique factorization domains and the Gauss lemma

The point of the Gauss lemma is that a polynomial f over the field of fractions F of a UFD R can be expressed as a rational number called the content of f times a polynomial over R called the primitive part. The point of the Gauss lemma is that it allows us to make sure that the content will in fact be an element of R.

The following lemma shows that in UFDs irreducibles are primes, but this is not true in general. (Counterexample in $\mathbb{Z}[\sqrt{-5}]$.)

Lemma 5.1. *If R is a UFD then irreducible elements are prime.*

Proof. If f is irreducible and $f|ab$ then f must be an element of the unique factorization of a or b. □

In fact, showing that irreducibles are prime would be enough for our purpose of showing that $F[x]$ is a UFD when F is a field. We shall be able to prove this (without the assumption of UFD as above) via Bachet-Bézout theorem; which we state first in its version for integer numbers:

Theorem 5.2 (Bachet-Bézout for integers)**.** *Let $a, b \in \mathbb{Z}$ (what is the essential property of $\mathbb{Z}$ that makes this true?). Then there exist $x, y \in \mathbb{Z}$ with*

$$ax + by = gcd(a, b)$$

Therefore, if $c \in \mathbb{Z}$ divides both a and b then c divides $gcd(a, b)$ as well.

Lemma 5.3. *Let $a, b, c \in \mathbb{Z}$. If $a|bc$ and $(a, b) = 1$, then $a|c$.*

Proof. By Theorem 5.2, there exist elements p, q such that $ap + bq = 1 \implies apc + bcq = c$, so that a divides both summands and thus divides c. □

Theorem 5.4 (Division algorithm for polynomials)**.** *Let F be a field. Given two polynomials $f, g \in F[x]$ there are two unique $q, r \in F[x]$ such that*

$$f = qg + r, \qquad deg r < deg g.$$

Remark. *We use the hypothesis that F is a field to take a fraction with denominator the leading coefficient of g; that is, the theorem is valid if the leading coefficient of g is a unit.*

Proof. We may suppose that $\deg f \geq \deg g$ for if not we just pick $q = 0$ and $r = f$. Now we use induction. If $\deg f = \deg g = 0$ then f and g are numbers and the result is obvious since F is a field.

If $\deg f > 0$ we do as follows. Suppose $\deg f = n$ and $\deg g = m$. Write $f(x) = a_n x^n + f_1(x)$ and $g(x) = b_m x^m + g_1(x)$. Notice that

$$\frac{a_n x^n}{b_m x^m} g(x) = a_n x^n + \frac{a_n}{b_m} x^{n-m} g_1(x)$$

so that $f(x) - \frac{a_n}{b_m} x^{n-m} g(x) = f_1(x) - \frac{a_n}{b_m} x^{n-m} g_1(x)$. This is a polynomial of strictly less degree than that of f, so that we can use induction hypothesis to write it as $qg + r$ with $\deg r < m$. Then

$$f(x) = g(x)\left(q(x) + \frac{a_n}{b_m} x^{n-m}\right) + r(x).$$

To prove uniqueness suppose that $f = q_1 g + r_1 = q_2 g + r_2$. Then

$$(q_1 - q_2)g = r_1 - r_2$$

Taking degrees we see that the degree of this polynomial should be, by the right-hand-side less than the degree of g, and by the left hand side more than the degree of g. Then the degree must be zero and $q_1 = q_2$, $r_1 = r_2$. □

Recall that the greatest common divisor of two polynomials f and g is the *monic* polynomial of least degree that divides both f and g.

Theorem 5.5 (Bachet-Bézout for polynomials over field)**.** *Let F be a field and $f, g \in F[x]$. There exist elements $p, q \in F[x]$ such that $fp + gq = gcd(f, g)$.*

Proof. Consider the set

$$I := \{fx + gy : x, y \in F[x]\}.$$

Let $d = fp + gq$ be the monic polynomial of least degree of the form $fx + gy$, for $x, y \in F[x]$. Notice that the existence of d monic comes from F being a field. We claim that $d = \gcd(f, g)$. Indeed, we first check by division algorithm that d divides both f and g: suppose that $f = dq + r$ with $\deg r < \deg d$. Then, if $r = f - dq = f(1 - xq) - yg$ is not zero, dividing by its leading coefficient gives an element in I of degree strictly smaller than the degree of d, a contradiction. Thus r is zero. The same argument shows that $d|g$, and we conclude that Thus $\deg d \leq \deg \gcd(f, g)$.

Now, since $\gcd(f, g)$ divides both f and g, it divides $d = xf + yg$. (Indeed, if $c := \gcd(f, g)$ is such that $ca = f, cb = g$ then $c(ap+bq) = cap+cbq = fp+gq = d$.) Thus $\deg d = \deg \gcd(f, g)$, and since both are monic we are done. □

Finally we obtain

Lemma 5.6. *Let F be a field. Irreducible elements of $F[x]$ are prime. That is, if $f|gh$ then $f|g$ or $f|h$ for any $f, g, h \in F[x]$.*

Proof. Let $d = \gcd(f, g)$. Then $dp = f$ and $dq = g$. If d is not 1 we get that p is a unit. Then gp is a multiple by a unit of g which is divided by f: $gp = dpq = fq$. That's good enough.

Now suppose that $d = 1$. Then by Bachet-Bézout Theorem 5.5 there are $p, q \in F[x]$ such that $fp + gq = 1$. Then $fph + gqh = h$. Since by hypothesis $f|gh$ we conclude that f divides both summands, so $f|h$. □

Applying this last lemma over and over again we get that if $f|f_1 \dots f_k$ then f must divide f_i for some i.

Lemma 5.7. *If F is a field then $F[x]$ is a UFD.*

Proof. The existence of the factorization is an easy induction on the degree of $f \in R[x]$. If f has degree zero, then we are done. If f has positive degree and is irreducible, we are done. If f has positive degree and it is reducible, i.e. $f = gh$, then both g and h have strictly smaller degree and we may apply induction hypothesis to obtain a decomposition of each factor into irreducible elements.

To prove uniqueness suppose that there exists an element in $F[x]$ that admits more than one factorization in irreducible elements up to multiplication by units. Choose f so that $\deg f$ is minimal among all such elements.

Write two factorizations of f in irreducible elements as $f_1 \dots f_k = f'_1 \dots f'_\ell$. Suppose that the factors are in ascending order of degree.

We have that $f_1|f'_1 \dots f_{k'}$, so that f_1 must divide some $f'_{i'}$ by Lemma 5.6. Since $f'_{i'}$ is irreducible and f_1 is not a unit, we conclude that $f_{i'} = f_1 u$ for some unit u.

Then we apply cancellation law using that $R[x]$ is a domain to obtain $uf_2 \dots f_k = f'_2 \dots f'_{k'}$ is a polynomial with two distinct factorizations. Since f is minimal among all elements that admit more than one factorization, we conclude that $k = k'$ and $f_i = f'_i$ for all i. □

Remark 5.8. Notice that the proof given for integers does not work identically, for in this case we cannot conclude that $f_1 = f'_1$ directly from putting the factors in order of degree (we can conclude that they have the same degree, but not that they arr the same polynomial!).

The true definition of content can be done in three steps:

Definition 5.9. (1) (Order of a fraction a at a prime p.) Let $a \in F$. If $p \in R$ is irreducible, the *order* of a at p to be the number r such that $a = p^r b$ for some fraction b that does not have p as factor in the numerator nor in the denominator. (To understand the point of the Gauss lemma, notice that the order can be a fraction, i.e. if p is a factor of the denominator.)

(2) (Order of a polynomial $f \in F[x]$ at a prime p.) The *order of $f \in F[x]$ at p* is the minimium order of p in any of the coefficients of f. (Defining this number as the **minimum** ensures that the primitive part of f (see below) has all coefficients in R. It also follows that the gcd of the coefficients of the primitive part is 1.)

(3) (Content of $f \in F[x]$) The *content* of f is the product of every irreducible factor p of f raised to its order.

(4) (Primitive polynomial.) A polynomial is called *primitive* if it has content 1.

As explained in the beginning of this section, the point of the Gauss lemma is that it will allow us to make sure that the content of f is an element of R, i.e. not a fraction.

Also, in the definition of order of a fraction a at a prime p, notice the order well-defined, i.e. unique, by the uniqueness of the factorization in R.

Lemma 5.10 (True Gauss lemma). *Let R be a UFD and F its fraction field. Let $f, g \in F[x]$. Then the $cont(fg) = cont(f)cont(g)$.*

This clearly implies that the product of two primitive polynomials being primitive, and the converse I think is true as well.

Proof. Since $\mathrm{cont}(bf) = b\mathrm{cont}(f)$ it's enough to suppose that f and g are primitive. Indeed, taking content of fg we obtain on one hand $\mathrm{cont}(fg)$ and on the other hand $\mathrm{cont}(\mathrm{cont}(f)\mathrm{pp}(f)\mathrm{cont}(g)\mathrm{pp}(g)) = \mathrm{cont}(f)\mathrm{cont}(g)\mathrm{cont}(\mathrm{pp}(f)\mathrm{pp}(g))$. Thus we would finish if we show that the product of two primitive polynomials is primitive.

Put another way, it's enough to show will show that if f, g are primitive (as are the primitive parts of f and g in the preceding paragraph) then fg is primitive. This means that I will show that any p is not a factor of all the coefficients in fg. A coefficient of fg looks as $c_j = \sum_{i=0}^{j} a_i b_{j-i}$. Since f, g are primitive then p cannot divide all a_i and all b_i. Thus we can pick the maximum a_s and the maximum b_t that p does not divide. Then the c_j containing the product $a_s b_t$ will not be divided by p, for p cannot divide $a_s b_t$ because it is prime, but will divide the remaining terms in the sum c_j; thus if p divided c_j it would also divide $a_s b_t$lmail. □

Lemma 5.11 (Gauss). *If R is a UFD then $R[x]$ is a UFD.*

Proof. Let $f \in R[x]$ be distinct from 0. Since $F[x]$ is UFD we can write $f = f_1 \dots f_k$. Notice that the primitive parts of the f_i coincide with the primitive part of the product $f_1 \dots f_k$ by the Gauss Lemma:

$$f = c(f_1 \dots f_k)\mathrm{pp}(f_1 \dots f_k),$$
$$f = c(f_1)\mathrm{pp}(f_1) \dots c(f_k)\mathrm{pp}(f_k)$$

and we cancel the content part dividing (using that we are in a field) by the Gauss Lemma.

We also apply the Gauss Lemma to conclude that $c(f) = c(f_1) \dots c(f_k)$, being the content of a polynomial with coefficients in R, must be in R as well, so that we can decompose it as a product of irreducibles since R is a UFD.

To obtain a factorization in irreducibles we only need to show that each of the $\text{pp}(f_i)$ is irreducible in $R[x]$. To see this suppose that $\text{pp}(f_i) = gh$. $c(f_i)\text{pp}(f_i) = f_i$ is irreducible in $F[x]$, so either $c(f_i)g$ or h is a unit of F. Then either g or h are in R. But the gcd of the coefficients of $\text{pp}(f_i)$ is 1, so, since we have factored an element of R from $\text{pp}(f_i)$, it must be 1.

The uniqueness of the factorization follows from the uniqueness of the factorization in $F[x]$, for another factorization in $R[x]$ would be a factorization in $F[x]$ Indeed, to see this suppose that $f = gh$ with $g, h \in F[x]$. Then take contents. The content of f must be a unit for otherwise f the principal part would have to be trivial, and f is not a constant. By the Gauss Lemma the contents of g and h are units. Then we are left with $f = \text{pp}(g)\text{pp}(h)$, an equation in $R[x]$ that makes either of the principal parts a unit of $R[x]$.

Then any factorization in $R[x]$ has the same number of factors, and any two factorizations are equal up to a fraction u, which is a unit of $F[x]$. We just need to make sure u is a unit of R. Write uniqueness of the factorization in $F[x]$ as: $f_1 = uf_1'$ and $f_i = f_i'$ for $i \neq 1$. It is clear that $u \in R$, since otherwise f_1 couldn't be a polynomial in $R[x]$. But since f_1 is irreducible in $R[x]$ and f_1' is not a unit of $R[x]$, we conclude that u is a unit of $R[x]$. □

Lemma 5.12. *In a UFD, irreducible elements generate prime ideals.*

Proof. Let f be irreducible. Suppose that $pq \in (f)$. Then $pq = fg$ for some $g \in R$. Then $p_1 \dots p_k q_1 \dots q_\ell = f g_1 \dots g_m$. But since f is irreducible and factorization is unique we conclude that f must be one of the p_i or one of the q_i. Then f divides p or q, i.e. either $p \in (f)$ or $q \in (f)$. □

6. Unique factorization domains (alternative approach)

Lemma 6.1. *$pp(f)$ is unique up to multiplication by unit.*

Proof. This follows from uniqueness up to units of gdc and lcm. □

Definition 6.2. If $f \in F[x]$, define its *primitive part* to be a primitive polynomial $\text{pp}(f)$ such that $c\text{pp}(f) = df$ where

- $d \in R$ is the minimum common factor of the denominators of the coefficients of f, which may be defined as the product of the least elements among all the factors (in their unique factorization) of the denominators such that $df \in R[x]$.
- $c \in R$ is the greatest common divisor of the coefficients of df, which may be defined as the product of the greatest number of common elements in the factorizations of each of the coefficients in df.

Lemma 6.3 (Gauss)**.** *Let R be a ring and F its field of fractions. A primitive polynomial $f \in R[x]$ is irreducible in $F[x]$ if and only if it is irreducible in $R[x]$.*

Proof. The direct implication is easy: suppose f is irreducible in $F[x]$ and let $f = gh$ for $g, h \in R[x]$. Then g, h are also in $F[x]$ so that either of them must be a unit of F, i.e. a fraction. But since they are polynomials in $R[x]$, then it must be an element of R. But since f is primitive we obtain a contradiction unless the number is a unit.

For the converse, suppose that f is irreducible in $R[x]$. To obtain a contradiction suppose that $f = gh$ in $F[x]$ with g, h not units in $F[x]$. Then $f = c\mathrm{pp}(f) = c\mathrm{pp}(g)\mathrm{pp}(h)$ by the True Gauss lemma. Notice that we cannot take primitive parts of g and h separately since this would give perhaps rational contents. □

Lemma 6.4. *If $f \in F[x]$ is irreducible (in $F[x]$), then its primitive part $pp(f)$ is irreducible in $R[x]$.*

Proof. Suppose that $\mathrm{pp}(f) = gh$ for two non-unit polynomials $g, h \in F[x]$. Multiplying by c as in Definition 6.2 we obtain $c\mathrm{pp}(f) = cgh \implies df = cgh \implies f = \frac{c}{d}gh$, a contradiction since f is irreducible in $F[x]$. This shows that $\mathrm{pp}(f)$ is irreducible in $F[x]$. By Gauss lemma, since $\mathrm{pp}(f)$ is irreducible in $F[x]$ and primitive, it must be irreducible in $R[x]$. □

Lemma 6.5. *If R then $R[x]$ is a UFD.*

Proof. Let $f \in R[x]$. Let c be the greatest common divisor of the coefficients of f, so that $f = cf'$. Factor f' in $F[x]$ as $f' = f'_1 \dots f'_k$. Take primitive parts to write $f = c'\mathrm{pp}(f'_1)\dots\mathrm{pp}(f'_k)$. By Lemma 6.4 each of the $\mathrm{pp}(f'_i)$ is primitive in $R[x]$. By the True Gauss lemma we get that $c' = c \in R$. Since R is a UFD we also obtain that c' may be factored into irreducible elements of R, which are also irreducible in $R[x]$.

Uniqueness of the factorization follows from uniqueness of the factorization in $F[x]$ and Gauss lemma: suppose that f may also be factored into irreducible elements of $R[x]$ as $g_1 \dots g_\ell$. We wish to show that this is a factorization in irreducible elements of $F[x]$, which we know to be unique up to multiplication by units of F. To show this we use the converse implication of Gauss lemma 6.3: after taking primitive parts to obtain $\mathrm{pp}(g_i)$, which are irreducible and primitive elements of $R[x]$, which must be irreducible in $F[x]$. Then $i = \ell$, the constants coincide and $\mathrm{pp}(g_i) = \mathrm{pp}(f_i)$. Since taking primitive part is unique up to multiplication by unit, we are done.

By induction on the degree of $f \in R[x]$. Write $f = cf'$ for $c = \gcd(\text{coefficients of } f)$. Then I claim that $f = cf'$ is a factorization of f into irreducible elements. f' is irreducible because it is linear and primitive; that is, writing $f' = c'f''$ is impossible because there is no way to factor a non-unit number from the coefficients of f'; indeed, in such case, cc' would be a *larger* common factor of f. Here I define larger as follows using that R is UFD: if $a = a_1 \dots a_k$ and $b = b_1 \dots b_\ell$ then the gdc is the product of all common factors of a and b.

To conclude our induction now suppose that degree-n elements have factorization and let f be of degree $n + 1$. If f is irreducible we are done. Otherwise f can be expressed as the product of two positive degree elements, each of which is expressed in a product of irreducibles. □

References