

A Primer on Sizes of Polynomials

Suppose p is a prime number. By the Fundamental Theorem of Arithmetic (unique factorization of integers), every non-zero integer n can be uniquely written in the form $n = p^k m$ where $p \nmid m$. This unique power k is called the *order of n at p* and denoted $\text{ord}_p(n)$. By convention, $\text{ord}_p(0) = \infty$.

Definition: Suppose $r/s \in \mathbb{Q}$, where $r, s \in \mathbb{Z}$. Then $\text{ord}_p(r/s) = \text{ord}_p(r) - \text{ord}_p(s)$.

Note how this definition really is ... a definition. In other words, it doesn't depend on how you write the rational number. For instance, $\text{ord}_p(1/2)$ really is the same as $\text{ord}_p(2/4)$ and $\text{ord}_p(17/34)$. This actually follows from the integer case of the following lemma.

Lemma 1: Suppose p is a prime and $a, b \in \mathbb{Q}$. Then

$$\text{ord}_p(ab) = \text{ord}_p(a) + \text{ord}_p(b).$$

Also,

$$\text{ord}_p(a + b) \geq \min\{\text{ord}_p(a), \text{ord}_p(b)\},$$

with equality if $\text{ord}_p(a) \neq \text{ord}_p(b)$.

Proof: This is obvious if either a or b is zero, so we will assume $ab \neq 0$.

First suppose $a, b \in \mathbb{Z}$. Write $a = p^{\text{ord}_p(a)} m_1$ and $b = p^{\text{ord}_p(b)} m_2$, where $p \nmid m_1$ and $p \nmid m_2$. Then $ab = p^{\text{ord}_p(a) + \text{ord}_p(b)} m_1 m_2$ where $p \nmid m_1 m_2$, which proves the first statement.

Without loss of generality, $\text{ord}_p(a) \leq \text{ord}_p(b)$. We then have

$$a + b = p^{\text{ord}_p(a)} (m_1 + p^{\text{ord}_p(b) - \text{ord}_p(a)} m_2),$$

and clearly $p \nmid (m_1 + p^{\text{ord}_p(b) - \text{ord}_p(a)} m_2)$ if $\text{ord}_p(b) > \text{ord}_p(a)$. Thus, the lemma is true for integers a and b .

Now suppose $a, b \in \mathbb{Q}$ and write $a = r/s$, $b = u/v$ for $r, s, u, v \in \mathbb{Z}$. Then $ab = (ru/sv)$ and by what we've already shown

$$\text{ord}_p(ab) = \text{ord}_p(ru) - \text{ord}_p(sv) = \text{ord}_p(r) + \text{ord}_p(u) - \text{ord}_p(s) - \text{ord}_p(v) = \text{ord}_p(a) + \text{ord}_p(b).$$

Further,

$$\begin{aligned}
 \text{ord}_p(sv(a+b)) &= \text{ord}_p(vr + su) \geq \min\{\text{ord}_p(vr), \text{ord}_p(su)\} \\
 &= \min\{\text{ord}_p(v) + \text{ord}_p(r), \text{ord}_p(s) + \text{ord}_p(u)\} \\
 &= (\text{ord}_p(s) + \text{ord}_p(v)) \min\{\text{ord}_p(r) - \text{ord}_p(s), \text{ord}_p(u) - \text{ord}_p(v)\} \\
 &= (\text{ord}_p(sv)) \min\{\text{ord}_p(a), \text{ord}_p(b)\},
 \end{aligned}$$

with equality if $\text{ord}_p(vr) \neq \text{ord}_p(su)$. By what we have already shown, this implies that $\text{ord}_p(a+b) \geq \min\{\text{ord}_p(a), \text{ord}_p(b)\}$, with equality if $\text{ord}_p(v) + \text{ord}_p(r) \neq \text{ord}_p(s) + \text{ord}_p(u)$. Thus, $\text{ord}_p(a+b) = \min\{\text{ord}_p(a), \text{ord}_p(b)\}$ if $\text{ord}_p(r) - \text{ord}_p(s) \neq \text{ord}_p(u) - \text{ord}_p(v)$, i.e., if $\text{ord}_p(a) \neq \text{ord}_p(b)$.

So the behavior of the ord_p function is somewhat reminiscent of the degree function. In fact, it behaves just like *minus* the degree function except the degree is a function on polynomials whereas ord_p is a function on \mathbb{Q} . Our goal is really to get a “size” for polynomials with properties similar to those of the degree function. But before we jump to that, a couple remarks are in order.

First of all, notice how $\text{ord}_p(r/s)$ will typically be 0; the only time it won't be zero is if p is a factor of either r or s . Second, r/s will be an integer if and only if $\text{ord}_p(r/s) \geq 0$ for all primes p .

Definition: If $P = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Q}[X]$, then

$$\text{ord}_p(P) = \min_{1 \leq i \leq n} \{\text{ord}_p(a_i)\}.$$

In other words, the order at p of a polynomial is defined to be the minimum of the orders at p of the coefficients. This is the same thing as the order of the greatest common divisor of the coefficients when $P \in \mathbb{Z}[X]$, which is the same as the highest power of p that divides all the coefficients (definition used in class, 2/26).

Remarks: Only the zero polynomial has order equal to ∞ . For any non-zero polynomial P , $\text{ord}_p(P) = 0$ for all but finitely many primes p . Also, P has integer coefficients if and only if $\text{ord}_p(P) \geq 0$ for all primes p .

The idea here is that the order at p behaves exactly like minus the degree function. Specifically, we have the following.

Lemma 2 (Gauss' Lemma): Suppose p is a prime number and $P, Q \in \mathbb{Q}[X]$. Then

$$\text{ord}_p(PQ) = \text{ord}_p(P) + \text{ord}_p(Q)$$

and

$$\text{ord}_p(P + Q) \geq \min\{\text{ord}_p(P), \text{ord}_p(Q)\},$$

with equality when $\text{ord}_p(P) \neq \text{ord}_p(Q)$.

Proof: Let n be the maximum of the degree of P and the degree of Q . Write

$$P = a_0 + a_1X + \cdots + a_nX^n, \quad Q = b_0 + b_1X + \cdots + b_nX^n.$$

Let l be the largest index i where $\text{ord}_p(P) = \text{ord}_p(a_i)$ and let k be the largest index j where $\text{ord}_p(Q) = \text{ord}_p(b_j)$. We then have $\text{ord}_p(a_i) \geq \text{ord}_p(a_l)$ for all i and $\text{ord}_p(a_i) > \text{ord}_p(a_l)$ for all $i > l$ (and similarly for the b_j 's). By Lemma 1, this implies that

$$\text{ord}_p(a_i b_j) = \text{ord}_p(a_i) + \text{ord}_p(b_j) > \text{ord}_p(P) + \text{ord}_p(Q)$$

if either $i > l$ or $j > k$, and

$$\text{ord}_p(a_i b_j) = \text{ord}_p(a_i) + \text{ord}_p(b_j) \geq \text{ord}_p(P) + \text{ord}_p(Q)$$

in general. Hence by Lemma 1

$$\text{ord}_p\left(\sum_{i=0}^m a_i b_{m-i}\right) \geq \text{ord}_p(P) + \text{ord}_p(Q)$$

for any $m \geq 0$. We also have

$$\text{ord}_p\left(\sum_{i=0}^{l+k} a_i b_{(l+k)-i}\right) = \text{ord}_p(P) + \text{ord}_p(Q),$$

since either $i > l$ or $(l+k) - i > k$ except for when $i = l$ (and then $(l+k) - i = k$). This proves the first statement.

Without loss of generality, we may assume $\text{ord}_p(P) \geq \text{ord}_p(Q)$. Since $\text{ord}_p(a_k) \geq \text{ord}_p(P) \geq \text{ord}_p(Q) = \text{ord}_p(b_k)$, by Lemma 1 $\text{ord}_p(a_k + b_k) \geq \text{ord}_p(b_k) = \text{ord}_p(Q)$, with equality if $\text{ord}_p(P) > \text{ord}_p(Q)$. Also, $\text{ord}_p(a_j + b_j) \geq \min\{\text{ord}_p(a_j), \text{ord}_p(b_j)\} \geq \text{ord}_p(Q)$ for all j . This proves the second statement.

Definition: Suppose $P \in \mathbb{Q}[X]$ is a non-zero polynomial. Then $\text{ord}_p(P) = 0$ for all but finitely many primes p ; denote them by p_1, \dots, p_n . The *content* of P , denoted $\text{cont}(P)$, is defined to be

$$\text{cont}(P) = p_1^{\text{ord}_{p_1}(P)} \cdots p_n^{\text{ord}_{p_n}(P)}.$$

Remark: It isn't difficult to check that $\text{cont}(P)$ is the greatest common divisor of the coefficients when $P \in \mathbb{Z}[X]$. Also, $\text{cont}(P) \in \mathbb{Z}$ if and only if $P \in \mathbb{Z}[X]$. Thus, P is *primitive* (the definition is in section 4.4 of the textbook) if and only if $\text{cont}(P) = 1$. What we're doing here is really just an elaboration of the book's approach.

Lemma 3: If $P, Q \in \mathbb{Q}[X]$ are non-zero polynomials, then $\text{cont}(PQ) = \text{cont}(P) \cdot \text{cont}(Q)$.

Proof: Just apply Lemma 2 to the finite collection of primes p where either $\text{ord}_p(P) \neq 0$ or $\text{ord}_p(Q) \neq 0$. Note how this certainly takes into account all primes where $\text{ord}_p(PQ) \neq 0$ by Lemma 2.

Definition: Suppose $P \in \mathbb{Q}[X]$ is a non-zero polynomial. Define

$$P^* = (\text{cont}(P))^{-1}P.$$

Lemma 4: Suppose $P \in \mathbb{Q}[X]$ is a non-zero polynomial. Then $\text{ord}_p(P^*) = 0$ for all primes p , i.e., $P^* \in \mathbb{Z}[X]$ is a primitive polynomial. Also, if Q is another non-zero polynomial, then $(PQ)^* = P^*Q^*$.

Proof: By definition we have $\text{ord}_p(\text{cont}(P)) = \text{ord}_p(P)$ for all primes p . We can view $(\text{cont}(P))^{-1}$ as a polynomial of degree 0. By Lemma 1, the order at p of $(\text{cont}(P))^{-1}$ is the negative of the order at p of the content of P . The first statement thus follows from Lemma 2. The last statement follows directly from Lemma 3 and the definitions.

Corollary to all this stuff: Suppose $P \in \mathbb{Q}[X]$ is a non-zero polynomial and write P as a product of irreducible polynomials:

$$P = P_1P_2 \cdots P_n.$$

Then

$$P^* = P_1^*P_2^* \cdots P_n^*.$$

In particular, if $P \in \mathbb{Z}[X]$, then P can be written uniquely as a product of its content and primitive irreducible polynomials:

$$P = \text{cont}(P)P_1^*P_2^* \cdots P_n^*.$$