

# THE GAUSS NORM AND GAUSS'S LEMMA

KEITH CONRAD

In algebra, the name “Gauss’s Lemma” is used to describe any of a circle of related results about polynomials with integral coefficients. Here are three.

The first result, which can be found in [1, p. 528], says that a factorization in  $\mathbf{Q}[T]$  of a polynomial in  $\mathbf{Z}[T]$  can be adjusted to be a factorization in  $\mathbf{Z}[T]$  just by scaling the factors.

**Theorem 1.** *If  $f(T) \in \mathbf{Z}[T]$  is nonzero and  $f(T) = g(T)h(T)$  in  $\mathbf{Q}[T]$  then  $f(T) = G(T)H(T)$  where  $G(T)$  and  $H(T)$  are in  $\mathbf{Z}[T]$ ,  $G$  is a scalar multiple of  $g$  in  $\mathbf{Q}[T]$  and  $H$  is a scalar multiple of  $h$  in  $\mathbf{Q}[T]$ .*

**Example 2.** Let  $f(T) = T^2 - 4$ . Then  $f(T) = (3T - 6)(T/3 - 2/3)$  is a factorization in  $\mathbf{Q}[T]$ . Multiplying the first factor by  $1/3$  and the second factor by  $3$ , we get the more familiar factorization  $f(T) = (T - 2)(T + 2)$  in  $\mathbf{Z}[T]$ .

The second result, which is in [3, p. 40], is about primitive polynomials. A polynomial in  $\mathbf{Z}[T]$  is called *primitive* when its coefficients are relatively prime when considered together. For example,  $6T^2 + 10T + 15$  is primitive; even though each pair of coefficients is not relatively prime, the triple of coefficients  $(6, 10, 15)$  is relatively prime and that makes the polynomial primitive.

**Theorem 3.** *If  $f(T)$  and  $g(T)$  are primitive in  $\mathbf{Z}[T]$  then  $f(T)g(T)$  is primitive.*

The third result was essentially stated by Gauss himself [2, Article 42].

**Theorem 4.** *If  $f(T)$  is monic in  $\mathbf{Z}[T]$  and  $f(T) = g(T)h(T)$  in  $\mathbf{Q}[T]$  where  $g(T)$  and  $h(T)$  are monic, then  $g(T)$  and  $h(T)$  are in  $\mathbf{Z}[T]$ .*

We will prove these theorems with an extension of the  $p$ -adic absolute value from  $\mathbf{Q}$  to  $\mathbf{Q}[T]$ .

**Definition 5.** For a polynomial  $f(T) = \sum a_n T^n$  in  $\mathbf{Q}[T]$  and a prime  $p$ , define the  $p$ -adic Gauss norm of  $f$  to be  $|f|_p = \max_n |a_n|_p$ .

In this definition we are not specifying the degree of the polynomial  $f$ , but it doesn’t matter since the maximum in the definition of  $|f|_p$  is unaffected by additional coefficients that are 0. If  $f(T) = c$  is constant then  $|f|_p = |c|_p$ , so  $|\cdot|_p$  on  $\mathbf{Q}[T]$  restricts to the  $p$ -adic absolute value on  $\mathbf{Q}$ .

**Example 6.** If  $f(T) = 6T^2 - (5/3)T + 4/7$ , we have  $|f|_2 = \max(1/2, 1, 1/4) = 1$ ,  $|f|_3 = \max(1/3, 3, 1) = 3$ ,  $|f|_5 = \max(1, 1/5, 1) = 1$ ,  $|f|_7 = \max(1, 1, 7) = 7$ , and  $|f|_p = 1$  for all  $p > 7$ . Note  $\prod_p |f|_p = 21$  and  $21f(T) = 126T^2 - 35T + 12$  is a scalar multiple of  $f(T)$  with integral coefficients that is primitive. This idea will be used later.

To get used to the meaning of the  $p$ -adic Gauss norms as  $p$  varies, we show how to use them to describe being primitive in  $\mathbf{Z}[T]$ .

**Theorem 7.** *A polynomial  $f(T)$  in  $\mathbf{Q}[T]$  is primitive in  $\mathbf{Z}[T]$  if and only if  $|f|_p = 1$  for all primes  $p$ .*

*Proof.* If  $f$  is primitive in  $\mathbf{Z}[T]$  then for each prime  $p$  we have  $|f|_p = 1$  because all the coefficients of  $f$  are integers (so  $|f|_p \leq 1$ ) and at least one of its coefficients is not divisible by  $p$  (so  $|f|_p = 1$ ).

Conversely, assume for each prime  $p$  that  $|f|_p = 1$ . Then each coefficient of  $f$  has  $p$ -adic absolute value at most 1 for all  $p$ , so each coefficient of  $f$  is a  $p$ -adic integer for all  $p$ . A rational number that is in  $\mathbf{Z}_p$  for all  $p$  is in  $\mathbf{Z}$ , so  $f(T) \in \mathbf{Z}[T]$ . If  $f(T)$  were not primitive then its coefficients would share a common prime factor  $p$  and then  $|f|_p < 1$  for that  $p$ . Therefore the assumption that  $|f|_p = 1$  for all  $p$  implies  $f$  is primitive.  $\square$

Clearly  $|f|_p \geq 0$  with equality if and only if  $f = 0$ , and easily  $|f + g|_p \leq \max(|f|_p, |g|_p)$  and  $|fg|_p \leq |f|_p |g|_p$  by the formulas for adding and multiplying polynomials together with the strong triangle inequality. Perhaps surprisingly,  $|\cdot|_p$  is actually multiplicative on  $\mathbf{Q}[T]$ .

**Theorem 8.** For  $f$  and  $g$  in  $\mathbf{Q}[T]$ ,  $|fg|_p = |f|_p |g|_p$ .

*Proof.* If  $f = 0$  or  $g = 0$  then the equality is obvious, so we can assume  $f$  and  $g$  each have some nonzero coefficients:  $|f|_p > 0$  and  $|g|_p > 0$ .

Write  $f(T) = \sum a_m T^m$  and  $g(T) = \sum b_n T^n$ . (We don't specify where the polynomials stop; coefficients equal 0 in large degrees.) Since  $|fg|_p \leq |f|_p |g|_p$ , to prove  $|fg|_p = |f|_p |g|_p$  we seek a coefficient in  $fg$  with absolute value  $|f|_p |g|_p$ . We will do this in two ways.

**Method 1:** Focus on where coefficients of maximal absolute value in  $f$  and  $g$  *first* occur.

Set  $|f|_p = |a_M|_p$  with  $M$  minimal and  $|g|_p = |b_N|_p$  with  $N$  minimal:  $|a_m|_p < |a_M|_p$  for  $m < M$  and  $|b_n|_p < |b_N|_p$  for  $n < N$ . (If either  $M$  or  $N$  is 0 then such an inequality is an empty condition.) We seek a coefficient in  $fg$  with absolute value  $|f|_p |g|_p$  and will find it in degree  $M + N$ .

The coefficient of  $T^{M+N}$  in  $fg$  is  $\sum_{m=0}^{M+N} a_m b_{M+N-m}$ . The term in this sum at  $m = M$  is  $a_M b_N$ . For  $0 \leq m < M$ ,

$$|a_m b_{M+N-m}|_p = |a_m|_p |b_{M+N-m}|_p \leq |a_m|_p |g|_p = |a_m|_p |b_N|_p < |a_M|_p |b_N|_p.$$

For  $M < m \leq M + N$  we have  $0 \leq M + N - m < N$ , so

$$|a_m b_{M+N-m}|_p = |a_m|_p |b_{M+N-m}|_p \leq |f|_p |b_{M+N-m}|_p = |a_M|_p |b_{M+N-m}|_p < |a_M|_p |b_N|_p.$$

Thus  $|a_m b_{M+N-m}|_p < |a_M b_N|_p$  for  $0 \leq m \leq M + N$  with  $m \neq M$ , so by the strong triangle inequality we get

$$\left| \sum_{m=0}^{M+N} a_m b_{M+N-m} \right|_p = |a_M b_N|_p = |a_M|_p |b_N|_p = |f|_p |g|_p.$$

**Method 2:** Focus on where coefficients of maximal absolute value in  $f$  and  $g$  *last* occur.

Now set  $|f|_p = |a_M|_p$  with  $M$  maximal and  $|g|_p = |b_N|_p$  with  $N$  maximal:  $|a_m|_p < |a_M|_p$  for  $m > M$  and  $|b_n|_p < |b_N|_p$  for  $n > N$ . We'll see that a coefficient in  $fg$  of  $p$ -adic absolute value  $|f|_p |g|_p$  occurs in degree  $M + N$ .

The coefficient of  $T^{M+N}$  in  $fg$  is  $\sum_{m=0}^{M+N} a_m b_{M+N-m}$  and the term in this sum at  $m = M$  is  $a_M b_N$ . If  $0 \leq m < M$  then  $M + N - m > N$ , so

$$|a_m b_{M+N-m}|_p = |a_m|_p |b_{M+N-m}|_p \leq |f|_p |b_{M+N-m}|_p = |a_M|_p |b_{M+N-m}|_p < |a_M|_p |b_N|_p.$$

For  $M < m \leq M + N$ ,

$$|a_m b_{M+N-m}|_p = |a_m|_p |b_{M+N-m}|_p \leq |a_m|_p |g|_p = |a_m|_p |b_N|_p < |a_M|_p |b_N|_p.$$

Thus  $|a_m b_{M+N-m}|_p < |a_M b_N|_p$  for  $0 \leq m \leq M+N$  with  $m \neq M$ , so by the strong triangle inequality we get

$$\left| \sum_{m=0}^{M+N} a_m b_{M+N-m} \right|_p = |a_M b_N|_p = |a_M|_p |b_N|_p = |f|_p |g|_p.$$

□

The proof of Theorem 8 did not need the coefficients to be rational: Definition 5 for the prime  $p$  makes sense on  $\mathbf{Q}_p[T]$ , not just  $\mathbf{Q}[T]$  (where  $p$  can vary), and Theorem 8 holds on  $\mathbf{Q}_p[T]$  by the same proof. While we only need one of the methods in the proof of Theorem 8, there are generalizations of Theorem 8 from polynomials to different types of  $p$ -adic power series – the formal power series  $\mathbf{Z}_p[[T]]$  and the restricted power series  $\mathbf{Q}_p\langle T \rangle$  – where one method works and the other doesn't, so both are worthwhile. Gauss himself used the first method (on polynomials).

**Remark 9.** We can extend the ordinary absolute value on  $\mathbf{Q}$  to  $\mathbf{Q}[T]$  in the same way as we did  $|\cdot|_p$  and the ordinary triangle inequality  $|f+g| \leq |f|+|g|$  trivially holds, but behavior under multiplication is bad:  $|T+1| = 1$  but  $|(T+1)^n| = |T^n + nT^{n-1} + \cdots + 1| \geq n$ , so  $|(T+1)^n| \rightarrow \infty$  as  $n \rightarrow \infty$ .

To prove Theorem 1 we use the following result that shows how to systematically scale a polynomial in  $\mathbf{Q}[T]$  to a primitive polynomial in  $\mathbf{Z}[T]$  using all the Gauss norms on  $\mathbf{Q}[T]$ .

**Lemma 10.** *For  $f(T) \in \mathbf{Q}[T]$  set  $A = \prod_p |f|_p$ . Then  $Af(T)$  is in  $\mathbf{Z}[T]$  and is primitive.*

The product over all  $p$  defining  $A$  makes sense since  $|f|_p = 1$  for all but finitely many  $p$ .

*Proof.* For each integer  $n$ , the fact that  $|p^n|_p = 1/p^n$  and  $|q^n|_p = 1$  for primes  $q \neq p$  tells us that  $|A|_p = |f|_p|p|_p = 1/|f|_p$ . Thus  $|Af|_p = |A|_p|f|_p = 1$  for all  $p$ , so  $Af(T)$  is primitive in  $\mathbf{Z}[T]$  by Theorem 7. □

**Proof of Theorem 1.** Let  $A = \prod_p |f|_p$ ,  $B = \prod_p |g|_p$ , and  $C = \prod_p |h|_p$ . Since  $|f|_p = |g|_p|h|_p$  for all  $p$ , taking the product of both sides over all  $p$  implies  $A = BC$ .

By Lemma 10, the polynomials  $F(T) = Af(T)$ ,  $G(T) = Bg(T)$ , and  $H(T) = Ch(T)$  are all in  $\mathbf{Z}[T]$ . From  $f = gh$  we get  $F(T)/A = (G(T)/B)(H(T)/C) = G(T)H(T)/BC = G(T)H(T)/A$ , so  $F(T) = G(T)H(T)$ . Thus

$$f(T) = \frac{1}{A}F(T) = \frac{1}{A}G(T)H(T).$$

The coefficients of  $f$  are integers, so  $1/|f|_p \in \mathbf{Z}$  for all  $p$  and thus  $1/A \in \mathbf{Z}$ . Therefore  $(1/A)G(T) \in \mathbf{Z}[T]$ , so renaming  $(1/A)G(T)$  as  $G(T)$  we are done.

**Proof of Theorem 3.** By  $(\Rightarrow)$  in Theorem 7,  $|f|_p = 1$  and  $|g|_p = 1$  for each prime  $p$ . Thus  $|fg|_p = |f|_p|g|_p = 1$  for all  $p$ , so  $fg$  is primitive by  $(\Leftarrow)$  in Theorem 7.

**Proof of Theorem 4.** A monic in  $\mathbf{Z}[T]$  is primitive, so  $|f|_p = 1$  for all  $p$ . Therefore  $|g|_p|h|_p = 1$ . Since  $g$  and  $h$  are monic,  $|g|_p \geq 1$  and  $|h|_p \geq 1$ , so the equation  $|g|_p|h|_p = 1$  implies  $|g|_p = 1$  and  $|h|_p = 1$  for all  $p$ . Thus  $g$  and  $h$  are in  $\mathbf{Z}[T]$  by  $(\Leftarrow)$  in Theorem 7.

## REFERENCES

- [1] D. A. Cox, *Galois Theory*, 2nd ed., Wiley, 2012.
- [2] C. F. Gauss, *Disquisitiones Arithmeticae*, Yale Univ. Press, 1966.
- [3] J. Rotman, *Galois Theory*, 2nd ed., Springer, 2013.