

### Factoring in $\mathbb{Z}[x]$

This is an alternate version of the Gauss Lemma.

An integer polynomial  $f(x) = a_n x^n + \cdots + a_1 x + a_0$  is called *primitive* if it is not a constant, and if the coefficients  $a_i$  have no common integer factor except  $\pm 1$ .

**Lemma 1.** *If prime integer  $p$  divides the product  $fg$  of two integer polynomials in the ring  $\mathbb{Z}[x]$ , then  $p$  divides  $f$  or  $p$  divides  $g$  in  $\mathbb{Z}[x]$ .*

*Proof.* To say  $p$  divides a polynomial  $f$  means that  $p$  divides each coefficient of this polynomial. Let  $\bar{f}$  denote the reduction of  $f$  modulo  $p$ , i.e., the corresponding polynomial in the ring  $\mathbb{F}_p[x]$ . To say that  $p$  divides  $f$  is the same as saying  $\bar{f} = 0$ . Because reduction modulo  $p$  is a homomorphism,  $\overline{fg} = \bar{f}\bar{g}$ . Because  $\mathbb{F}_p[x]$  is a domain,  $\overline{fg} = 0$  implies that either  $\bar{f} = 0$  or  $\bar{g} = 0$ .  $\square$

**Theorem 1.** *Let  $f$  be a primitive polynomial, and let  $g$  be an integer polynomial. If  $f$  divides  $g$  in  $\mathbb{Q}[x]$ , then  $f$  divides  $g$  in  $\mathbb{Z}[x]$ .*

*Proof.* If  $f$  divides the integer polynomial  $g$  in  $\mathbb{Q}[x]$ , then we may write  $g = fq$ , where  $q \in \mathbb{Q}[x]$ . Clearing the denominators in  $q$  yields an equation of the form  $dg = fh$ , where  $d$  is a positive integer and  $h = dq \in \mathbb{Z}[x]$ . Let  $p$  be a prime factor of  $d$ . By the lemma,  $d$  divides one of the terms  $f, h$  on the right side of the equation. Since  $f$  is primitive,  $p$  does not divide  $f$ . So  $p$  divides  $h$ . We cancel  $p$  from  $d$  and  $h$  and proceed by induction. In the end, we are left with  $d = 1$  and  $g = fh$ , as required.  $\square$

**Lemma 2.** *Let  $f$  be an irreducible element of  $\mathbb{Z}[x]$ . Then either  $f$  is a primitive polynomial which is irreducible in  $\mathbb{Q}[x]$ , or else  $f$  is a prime integer.*

*Proof.* It is clear that the irreducible elements of  $\mathbb{Z}[x]$  of degree zero are the prime integers, and that a polynomial of positive degree which is irreducible is primitive. Suppose that  $g$  is primitive and not irreducible in  $\mathbb{Q}[x]$ . Then  $g$  has a proper factor  $f$  in  $\mathbb{Q}[x]$ , which we may take to be primitive. Theorem 1 shows that  $f$  divides  $g$  in  $\mathbb{Z}[x]$ , hence that  $g$  is not irreducible in this ring either.  $\square$

**Theorem 2.** *The ring  $\mathbb{Z}[x]$  is a unique factorization domain.*

*Proof.* It is clear that existence of factorizations holds in  $\mathbb{Z}[x]$ . We must show that every irreducible element  $f$  of  $\mathbb{Z}[x]$  is a prime element of this ring. This is Lemma 1 if  $f$  is a prime integer. Otherwise,  $f$  is an irreducible primitive polynomial. If  $f$  divides the product  $gh$  in  $\mathbb{Z}[x]$ , then because  $\mathbb{Q}[x]$  is a unique factorization domain and  $f$  is also irreducible in  $\mathbb{Q}[x]$ ,  $f$  divides  $g$  or  $h$  in that ring. Theorem 1 shows that  $f$  divides  $g$  or  $h$  in  $\mathbb{Z}[x]$  as well.  $\square$