

Either  $a_n = 0$  or  $b_m = 0$ . Suppose  $b_m = 0$ . Then you need to have  $(a(\lambda) + a_n \lambda^n) b(\lambda) = 0$ . By induction, one of these polynomials in the product is 0. If  $b(\lambda) \neq 0$ , then this shows  $a_n = 0$  and  $a(\lambda) = 0$  so  $f(\lambda) = 0$ . If  $b(\lambda) = 0$ , then  $g(\lambda) = 0$ . The argument is the same if  $a_n = 0$ . ■

**Lemma 2.14.3** *Let  $f(\lambda)$  and  $g(\lambda) \neq 0$  be polynomials. Then there exist polynomials,  $q(\lambda)$  and  $r(\lambda)$  such that*

$$f(\lambda) = q(\lambda)g(\lambda) + r(\lambda)$$

where the degree of  $r(\lambda)$  is less than the degree of  $g(\lambda)$  or  $r(\lambda) = 0$ . These polynomials  $q(\lambda)$  and  $r(\lambda)$  are unique.

**Proof:** Suppose that  $f(\lambda) - q(\lambda)g(\lambda)$  is never equal to 0 for any  $q(\lambda)$ . If it is, then the conclusion follows. Now suppose

$$r(\lambda) = f(\lambda) - q(\lambda)g(\lambda) \quad (*)$$

where the degree of  $r(\lambda)$  is as small as possible. Let it be  $m$ . Suppose  $m \geq n$  where  $n$  is the degree of  $g(\lambda)$ . Say  $r(\lambda) = b\lambda^m + a(\lambda)$  where  $a(\lambda)$  is 0 or has degree less than  $m$  while  $g(\lambda) = \hat{b}\lambda^n + \hat{a}(\lambda)$  where  $\hat{a}(\lambda)$  is 0 or has degree less than  $n$ . Then

$$r(\lambda) - \frac{b}{\hat{b}}\lambda^{m-n}g(\lambda) = b\lambda^m + a(\lambda) - \left(b\lambda^m + \frac{b}{\hat{b}}\lambda^{m-n}\hat{a}(\lambda)\right) = a(\lambda) - \tilde{a}(\lambda),$$

a polynomial having degree less than  $m$ . Therefore,

$$a(\lambda) - \tilde{a}(\lambda) = \overbrace{(f(\lambda) - q(\lambda)g(\lambda))}^{=r(\lambda)} - \frac{b}{\hat{b}}\lambda^{m-n}g(\lambda) = f(\lambda) - \hat{q}(\lambda)g(\lambda)$$

which is of the same form as  $*$  having smaller degree. However,  $m$  was as small as possible. Hence  $m < n$  after all.

As to uniqueness, if you have  $r(\lambda), \hat{r}(\lambda), q(\lambda), \hat{q}(\lambda)$  which work, then you would have  $(\hat{q}(\lambda) - q(\lambda))g(\lambda) = r(\lambda) - \hat{r}(\lambda)$ . Now if the polynomial on the right is not zero, then neither is the one on the left. Hence this would involve two polynomials which are equal although their degrees are different. This is impossible. Hence  $r(\lambda) = \hat{r}(\lambda)$  and so, the above lemma gives  $\hat{q}(\lambda) = q(\lambda)$ . ■

**Definition 2.14.4** *Let all coefficients of all polynomials come from a given field  $\mathbb{F}$ . For us,  $\mathbb{F}$  will be the real numbers  $\mathbb{R}$ . Let  $p(\lambda) = a_n \lambda^n + \dots + a_1 \lambda + a_0$  be a polynomial. Recall it is called monic if  $a_n = 1$ . If you have polynomials*

$$\{p_1(\lambda), \dots, p_m(\lambda)\},$$

the greatest common divisor  $q(\lambda)$  is the monic polynomial which divides each,  $p_k(\lambda) = q(\lambda)l_k(\lambda)$  for some  $l_k(\lambda)$ , written as  $q(\lambda)/p_k(\lambda)$  and if  $\hat{q}(\lambda)$  is any polynomial which divides each  $p_k(\lambda)$ , then  $\hat{q}(\lambda)/q(\lambda)$ . A set of polynomials

$$\{p_1(\lambda), \dots, p_m(\lambda)\}$$

is relatively prime if the greatest common divisor is 1.

**Lemma 2.14.5** *There is at most one greatest common divisor.*

**Proof:** If you had two,  $\hat{q}(\lambda)$  and  $q(\lambda)$ , then  $\hat{q}(\lambda)/q(\lambda)$  and  $q(\lambda)/\hat{q}(\lambda)$  so  $q(\lambda) = \hat{q}(\lambda)\hat{l}(\lambda) = q(\lambda)l(\lambda)\hat{l}(\lambda)$  and now it follows, since both  $\hat{q}(\lambda)$  and  $q(\lambda)$  are monic that  $\hat{l}(\lambda)$  and  $l(\lambda)$  are both equal to 1. ■

The next proposition is remarkable. It describes the greatest common divisor in a very useful way.