Proposition 2.14.6 *The greatest common divisor of* $\{p_1(\lambda), \cdots, p_m(\lambda)\}$ *exists and is characterized as the monic polynomial of smallest degree equal to an expression of the form*

$$\sum_{k=1}^{m} a_k(\lambda) p_k(\lambda), \text{ the } a_k(\lambda) \text{ being polynomials.} \tag{2.1}$$

Proof: First I need show that if $q(\lambda)$ is monic of the above form with smallest degree, then it is the greatest common divisor. If $q(\lambda)$ fails to divide $p_k(\lambda)$, then $p_k(\lambda) = q(\lambda) l(\lambda) + r(\lambda)$ where the degree of $r(\lambda)$ is smaller than the degree of $q(\lambda)$. Thus,

$$r(\lambda) = p_k(\lambda) - l(\lambda) \sum_{k=1}^{m} a_k(\lambda) p_k(\lambda)$$

which violates the condition that $q(\lambda)$ has smallest degree. Thus $q(\lambda) / p_k(\lambda)$ for each k. If $\hat{q}(\lambda)$ divides each $p_k(\lambda)$ then it must divide $q(\lambda)$ because $q(\lambda)$ is given by 2.1. Hence $q(\lambda)$ is the greatest common divisor.

Next, why does such greatest common divisor exist? Simply pick the monic polynomial which has smallest degree which is of the form $\sum_{k=1}^{m} a_k(\lambda) p_k(\lambda)$. Then from what was just shown, it is the greatest common divisor. ■

Proposition 2.14.7 *Let* $p(\lambda)$ *be a polynomial. Then there are polynomials* $p_i(\lambda)$ *such that*

$$p(\lambda) = a \prod_{i=1}^{m} p_i(\lambda)^{m_i} \tag{2.2}$$

where $m_i \in \mathbb{N}$ *and* $\{p_1(\lambda), \cdots, p_m(\lambda)\}$ *are monic and relatively prime. Every subset of* $\{p_1(\lambda), \cdots, p_m(\lambda)\}$ *having at least 2 elements is also relatively prime.*

Proof: If there is no polynomial of degree larger than 0 dividing $p(\lambda)$, then we are done. Simply pick a such that $p(\lambda)$ is monic. Otherwise $p(\lambda) = a p_1(\lambda) p_2(\lambda)$ where $p_i(\lambda)$ is monic and each has degree at least 1. These could be the same polynomial. If some nonconstant polynomial divides each $p_i(\lambda)$, factor further. Continue doing this. Eventually the process must end with a factorization as described in 2.2 because the degrees of the factors are decreasing. The claim about the subsets is clear because each polynomial is irreducible so the only monic polynomial dividing any of them is itself and 1. ■

2.15 The Cauchy Schwarz Inequality

This fundamental inequality takes several forms. I will present the version first given by Cauchy although I am not sure if the proof is the same.

Proposition 2.15.1 *Let* z_j, w_j *be complex numbers. Then*

$$\left| \sum_{j=1}^{p} z_j \overline{w_j} \right| \leq \left(\sum_{j=1}^{p} |z_j|^2 \right)^{1/2} \left(\sum_{j=1}^{p} |w_j|^2 \right)^{1/2}$$

Proof: First note that $\sum_{j=1}^{p} z_j \overline{z_j} = \sum_{j=1}^{p} |z_j|^2 \geq 0$. Next, if $a + ib$ is a complex number, consider $\theta = 1$ if both a, b are zero and $\theta = \frac{a - ib}{\sqrt{a^2 + b^2}}$ if the complex number is not zero. Thus, in either case, there exists a complex number θ such that $|\theta| = 1$ and $\theta(a + ib) = |a + ib| \equiv \sqrt{a^2 + b^2}$. Now let $|\theta| = 1$ and

$$\theta \sum_{j=1}^{p} z_j \overline{w_j} = \left| \sum_{j=1}^{p} z_j \overline{w_j} \right|$$