Euclidean algorithm

Theorem

Let A be a commutative ring. Let $f, g \in A[X]$ be polynomials in one variable of degrees ≥ 0. Assume that the leading coefficient of f is a unit. There exists unique polynomials $q, r \in A[X]$ such that

$$g = fq + r$$

and $\deg r < \deg f$.

We adopt the convention then $\deg(0) = -\infty$.

Existence

If $\deg g < \deg f$, then $(q, r) = (0, g)$ is the unique pair satisfying the condition. So Assume $\deg g \geq \deg f$. Write

$$f = aX^{\deg f} + f_1$$

where $\deg f_1 < \deg f$ and $a \in A^\times$. Similarly, write

$$g = bX^{\deg g} + g_1$$

with $\deg g_1 < \deg g$. Then,

$$\deg\left(g - ba^{-1}f \cdot X^{\deg g - \deg f}\right) < \deg(g)$$

Replace g by

$$g' := g - ba^{-1}f \cdot X^{\deg g - \deg f}$$

and repeat this process.

Uniqueness

Suppose we have two equations

$$g = fq + r$$
$$g = fq' + r'$$

with $\deg r$, $\deg r' < \deg f$. Taking the diffrence, we get

$$f(q - q') = r - r'.$$

Considering the degree, we get

$$f(q - q') = 0$$

Since $f = aX^{\deg f} + f_1$ with $\deg f_1 < \deg f$ and a is a non-zero-divisor, f is not a zero-divisor in $A[X]$. We conclude that $q = q'$ and $r = r'$.

Question

From this, deduce Theorem 1.4 in Lang's Algebra, p. 175.