Division Algorithm. Let $F[x]$ be a polynomial ring, where F is any field, such as $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$. The long division algorithm allows us to divide a polynomial $a(x)$ by $b(x)$ to get a quotient polynomial $q(x)$ with remainder $r(x)$:

$$a(x) = q(x)b(x) + r(x) \quad \text{with} \quad \deg r(x) < \deg b(x) \text{ or } r(x) = 0.$$

Apart from an algorithm, the existence and uniqueness of such $q(x), r(x)$ can be proved just as for division of integers.

Euclidean Algorithm.

We say one polynomial *divides* another, $c(x) \mid a(x)$, when $a(x) = c(x)q(x)$ for some polynomial $q(x) \in F[x]$; this just means the remainder of $a(x) \div c(x)$ is $r(x) = 0$. Equivalently, we say $c(x)$ is a *factor* or *divisor* of $a(x)$. Multiplying by a non-zero constant $u \in F$ has no effect on divisibility: if $c(x)$ is a factor of $a(x)$, then so is $u\,c(x)$, since:

$$a(x) = c(x)q(x) \quad \Longleftrightarrow \quad a(x) = u\,c(x) \cdot \tfrac{1}{u} q(x).$$

In fact u is a unit in $F[x]$, taking the role of ± 1 in the integer ring $\mathbb{Z}$.

For $a(x), b(x) \in F[x]$, their *greatest common divisor* $d(x) = \gcd(a(x), b(x))$ is a highest-degree polynomial dividing both $a(x)$ and $b(x)$.

EXAMPLE: In $\mathbb{Q}[x]$, the divisors of $a(x) = 9x^2 - 4$ are:

$$u,\ u\,(3x{-}2),\ u\,(3x{+}2),\ u\,(9x^2{-}4)$$

for any non-zero constant $u \in F$. The divisors of $b(x) = 3x^2 + 2x$ are:

$$u,\ u\,x,\ u\,(3x{+}2),\ u\,(3x^2{+}2x).$$

Thus $d(x) = \gcd(a(x), b(x)) = u\,(3x{+}2)$, which is unique except for the constant multiple. If we choose $u = \frac{1}{3}$ so as to make the leading coefficient equal to 1, we get the unique $d(x) = \frac{1}{3}(3x{+}2) = x{+}\frac{2}{3}$.

The Euclidean Algorithm is an efficient method to find $\gcd(a, b)$ for $\deg a(x) \geq \deg b(x)$ by repeated division with remainder, which works just as for integers.

Example. Find $d(x) = \gcd(a(x), b(x))$ for:

$$a(x) = 6x^4 + 2x^3 + 5x^2 + 3x + 2 \quad , \quad b(x) = 2x^2 + 1.$$

Repeated long division gives:

$$\begin{aligned}
a(x) &= (3x^2{+}x{+}1)\,b(x) + r_1(x) \quad \text{where} \quad r_1(x) = 2x{+}1 \\
b(x) &= (x{-}\tfrac{1}{2})\,r_1(x) + r_2(x) \quad \text{where} \quad r_2(x) = \tfrac{3}{2} \\
r_1(x) &= (\tfrac{4}{3}x{+}\tfrac{2}{3})\,r_2(x) + 0\,.
\end{aligned}$$

The gcd is the last non-zero remainder: $d(x) = r_2(x) = \frac{3}{2}$, which we can multiply by any non-zero constant u.

Given $r_{-1}(x) = a(x)$, $r_0(x) = b(x)$, $r_1(x), \ldots, r_i(x)$, the iterative rule is: $r_{i-1}(x) = q_{i+1}(x)r_i(x) + r_{i+1}(x)$ with $\deg r_i(x) > \deg r_{i+1}(x)$, ending when we reach $r_{i+1}(x) = 0$.

Extended Euclidean Algorithm

For $\gcd(a(x), b(x)) = d(x)$, we compute polynomials $f(x), g(x) \in F[x]$ with:

$$d(x) \;=\; f(x)a(x) + g(x)b(x).$$

Continuing our example, we solve for the the Euclidean algorithm remainders:

$$\begin{aligned} r_2(x) &= b(x) - (x-\tfrac{1}{2})\, r_1(x) \\ r_1(x) &= a(x) - (3x^2+x+1)\, b(x). \end{aligned}$$

Substituting the second equation into the first:

$$\begin{aligned} d(x) \;=\; r_2(x) &= b(x) - (x-\tfrac{1}{2})\, r_1(x) \\ &= b(x) - (x-\tfrac{1}{2})\,\big(a(x) - (3x^2+x+1)\, b(x)\big) \\ &= -(x-\tfrac{1}{2})\, a(x) + \big(1+(x-\tfrac{1}{2})(3x^2+x+1)\big)\; b(x) \\ \tfrac{3}{2} &= (-x+\tfrac{1}{2})\, a(x) + (3x^3-\tfrac{1}{2}x^2+\tfrac{1}{2}x+\tfrac{1}{2})\, b(x). \end{aligned}$$

To tidy this, we can multiply by $u = \frac{2}{3}$ to make $u\, d(x) = 1$:

$$1 \;=\; (-\tfrac{2}{3}x+\tfrac{1}{3})\, a(x) + (2x^3-\tfrac{1}{3}x^2+\tfrac{1}{3}x+\tfrac{1}{3})\, b(x).$$

Claim: $d(x) = r_2(x)$ is indeed the greatest common divisor.

We first prove that $d(x)$ must divide both $a(x)$ and $b(x)$. From the end of the Euclidean algorithm, we get $d(x) \,|\, d(x) = r_2(x)$ and $d(x) \,|\, q_3(x)r_2(x) = r_1(x)$; proceeding backward we get:

$$d(x) \mid q_2(x)r_1(x) + r_2(x) = b(x).$$

$$d(x) \mid q_1(x)a(x) + r_1(x) = a(x).$$

Therefore, $d(x)$ is *some* common divisor of $a(x), b(x)$. (Of course, here $d(x) = \frac{3}{2}$ divides any polynomial, but the argument illustrates the general case.)

Finally, we prove $d(x)$ is the *greatest* common divisor of $a(x), b(x)$. Suppose that $c(x)$ is any common divisor, so $c(x) \,|\, a(x)$ and $c(x) \,|\, b(x)$. Then clearly $c(x) \mid f(x)a(x) + g(x)b(x) = d(x)$, so that any common divisor $c(x)$ is also a divisor of $d(x)$, making $d(x)$ the greatest common divisor.

Irreducible Polynomials.

Just as for integers, a non-trivial factorization of a polynomial $f(x)$ writes it as the product of smaller-degree polynomials in $F[x]$:

$$f(x) \;=\; g(x)h(x) \quad \text{for} \quad \deg g(x), \deg h(x) < \deg f(x).$$

Factoring out a non-zero constant $u \in F$ from $f(x) = u \cdot \frac{1}{u} f(x)$ does not count as a factorization, since the second factor is not of smaller degree: $\deg \frac{1}{u} f(x) = \deg f(x)$. If $f(x) = u$ is itself a non-zero constant, then no non-trivial factorization is possible.

Repeated factorization must end, since the degrees of the factors keep getting smaller. The process ends with polynomials $p(x)$ which have no divisors except a constant u and $u\,p(x)$: we call these *irreducible* polynomials, analogous to prime numbers. Constant functions do *not* count as irreducibles.

The analog of the Prime Divisibility Property ([H] Thm 1.5 p. 18) is:

THEOREM: If $p(x)$ is an irreducible polynomial with $p(x) \mid a(x)b(x)$, then $p(x) \mid a(x)$ or $p(x) \mid b(x)$.

Proof: Let $p(x)$ be an irreducible polynomial with $p(x) \mid a(x)b(x)$. If $p(x) \mid a(x)$, the conclusion holds, and we are done.

If $p(x)$ is not a divisor of $a(x)$, and $p(x)$ has no other non-trivial divisors, then $p(x)$ and $a(x)$ have greatest common divisor $d(x) = 1$. The Extended Euclidean Algorithm gives $f(x)p(x) + g(x)a(x) = 1$. Multiplying by $b(x)$:

$$p(x) \mid f(x)p(x)b(x) + g(x)a(x)b(x) = b(x).$$

That is, $p(x) \mid b(x)$, and the conclusion holds in this case also.

Unique Factorization Theorem: In a polynomial ring $F[x]$, any polynomial $f(x)$ with $\deg f(x) > 1$ can be factored into irreducible polynomials in only one way, unique except for reordering the factors, and multiplying the factors by non-zero constants.

Proof: As we have seen, it is always possible to factor $f(x)$ until the factors are irreducible. Suppose we had two factorizations into irreducible polynomials:

$$f(x) \;=\; p_1(x) \cdots p_\ell(x) \;=\; q_1(x) \cdots q_m(x).$$

Since $p_1(x)$ divides the product $q_1(x)q_2(x) \cdots q_m(x)$, by the Prime Divisibility Property, either $p_1(x) \mid q_1(x)$ or $p_1(x) \mid q_2(x) \cdots q_m(x)$. In the second case, we repeat this argument until we finally find $p_1(x) \mid q_j(x)$ for some $q_j(x)$. Since $p_1(x)$ and $q_j(x)$ are both irreducible, this means $q_j(x) = u_1\, p_1(x)$ for some non-zero constant $u_1 \in F$. Let us reorder the factors $q_1, \ldots, q_m$ so that $q_j = q_1$ is at the beginning, with $q_1(x) = u_1\, p_1(x)$, and our equation becomes:

$$p_1(x)\, p_2(x) \cdots p_\ell(x) \;=\; u_1\, p_1(x)\, q_2(x) \cdots q_m(x).$$

Cancelling $p_1(x)$ from both sides gives:

$$p_2(x) \cdots p_\ell(x) \;=\; u_1\, q_2(x) \cdots q_m(x).$$

Now we perform the same process repeatedly, cancelling $p_2(x), \ldots, p_\ell(x)$, until finally we are left with only some extra q_i factors if $\ell < m$:

$$1 \;=\; u_1 u_2 \cdots u_\ell\, q_{\ell+1}(x) \cdots q_m(x).$$

However, the last factors $q_{\ell+1}(x) \cdots q_m(x)$ cannot be present, since an irreducible polynomial $q_j(x)$ is not constant, not invertible, and cannot multiply to produce 1.

Therefore $\ell = m$, and we can rearrange the $q_i(x)$'s so that $q_i(x) = u_i\, p_i(x)$ for non-zero constants $u_i \in F$. This is what we wanted to show.