Remark For a field K, the Euclidean Algorithm and the Extended Euclidean Algorithm can also be considered in the ring $K[t]$.

Example In $\mathbb{Q}[t]$ we consider

$$\begin{cases} f = t^2 - 3t + 2 \\ g = t^3 - t^2 - t + 1 \end{cases}$$

We want to determine $\gcd(f,g)$ and polynomials $a, b \in \mathbb{Q}[t]$ satisfying $a \cdot f + b \cdot g = \gcd(f,g)$.

$$\begin{array}{l} -\left(t^3 - t^2 - t + 1\right) : \left(t^2 - 3t + 2\right) = t + 2 \\ \underline{\; t^3 - 3t^2 + 2t \;} \\ \quad -2t^2 - 3t + 1 \\ \quad \underline{-2t^2 - 6t + 4} \\ \qquad\qquad 3t - 3 \end{array}$$

$$\begin{cases} f = t^2 - 3t + 2 \\ (-t-2)f + g = 3t - 3 \end{cases}$$

$$\begin{cases} 3f = 3t^2 - 9t + 6 \\ (-t-2)f + g = 3t - 3 \end{cases}$$

$$\begin{array}{r|l} (3t^2 - 9t + 6) & (3t - 3) \\ -(3t^2 - 3t) & t - 2 \\ \hline -6t + 6 & \\ -(-6t + 6) & \\ \hline 0 & \end{array}$$

$$\begin{cases} (3 - (-t-2)(t-2))f - (t-2)g = 0 \\ (-t-2)f + g = 3t - 3 \end{cases}$$

$$3 + (t+2)(t-2) = 3 + t^2 - 4 = t^2 - 1$$

$$\begin{cases} (t^2-1)f - (t-2)g = 0 \\ -(t+2)f + g = 3(t-1) \end{cases}$$

$\Rightarrow \gcd(f, g) = 3(t-1)$

It's defined up to a constant multiple

$$a \cdot f + b \cdot g = 3 \cdot (t-1)$$

for $a = -(t+2)$ and $b = 1$

Def Let K be a field and $g \in K[t]$ a polynomial of degree $\deg g \geq 1$. For $f \in K[t]$ we introduce the coset of f modulo g as

$$[f]_g := \{ h \in K[t] : f - h \text{ is divisible by } g \}$$

If f and h are such that $f-h$ is divisible by g, then f and h are called congruent modulo g; this is denoted as $f \equiv h \pmod g$.

We introduce the addition and multiplication of cosets by:

$$[a]_g + [b]_g := [a+b]_g,$$

$$[a]_g \cdot [b]_g := [a \cdot b]_g$$

for $a, b \in K[t]$.

By $K[t]/g$ we denote the set of all cosets of polynomials in $K[t]$ modulo g. That is:

$$K[t]/g := \{ [f]_g : f \in K[t] \}.$$

Proposition 24 Let K be a field and $g \in K[t]$ a polynomial of degree $\deg(g) \geq 1$. Then $(K[t]/g, +, \cdot)$ is a unitary commutative ring.

We omit the proof.

Example $g = t^2 - 2 \in \mathbb{Q}[t]$

$R = \mathbb{Q}[t]/g$.

Let $\alpha := [t]_g$.

What is $\alpha^2 - 2$ $= \alpha \cdot \alpha - [2]$

$= [t] \cdot [t] - [2]$

$= [t^2] - [2]$

$= [t^2 - 2]$

$= [0] = 0$.

Some random calculations:

$(1+\alpha)\cdot(2+\alpha)$ $= 2 + \alpha + 2\alpha + \alpha^2$

$= 2 + 3\alpha + \alpha^2$

$= 4 + 3\alpha$

$(1+\sqrt{2})\cdot(2+\sqrt{2}) = 4+3\sqrt{2}$

$(1+\alpha)^{-1}$ exists? $\quad (1+\alpha)^{-1} = \alpha - 1.$

$\alpha^2 = 2 \Rightarrow$

$\frac{1}{2}\alpha^2 = 1 \Rightarrow$

$\alpha^{-1} = \frac{1}{2}\alpha.$

$$\frac{1}{1+\sqrt{2}} = \frac{1-\sqrt{2}}{(1+\sqrt{2})(1-\sqrt{2})} = \frac{1-\sqrt{2}}{1-2} = \sqrt{2}-1$$

$(2+3\alpha)^{-1}$ exists?

$$\frac{1}{2+3\alpha} = \frac{2-3\alpha}{(2+3\alpha)(2-3\alpha)} = \frac{2-3\alpha}{4-9\alpha^2} = \frac{2-3\alpha}{4-9\cdot 2}$$

$$= \frac{3\alpha-2}{14} = \frac{3}{14}\alpha - \frac{2}{14} = \frac{3}{14}\alpha - \frac{1}{7}$$

$(2+3\alpha)^{-1} = \frac{1}{14}(3\alpha-2).$

$(5+\alpha)^{-1}$ exists?

It turns out that $\mathbb{R}$ is a field.

Example $g = t^2 - 1 \in \mathbb{Q}[t]$

$R := \mathbb{Q}[t]/g$

$\alpha := [t]_g$

$\alpha^2 - 1 = 0 \Rightarrow \alpha^2 = 1.$

Is $\alpha - 1$ invertible?

$(\alpha - 1) \cdot (\alpha + 1) = \alpha^2 - 1 = 0$ $\Rightarrow$ $\alpha - 1$ is a zero divisor in R and so not invertible.

($\alpha - 1 \neq 0$, $\alpha + 1 \neq 0$)

$\Rightarrow$ R is not a field.

Is α invertible

$\alpha \cdot \alpha = 1 \Rightarrow \alpha^{-1} = \alpha$

Is $2+\alpha$ invertible?

$$(2+\alpha)\cdot\frac{2-\alpha}{3} = \frac{4-\alpha^2}{3} = \frac{4-1}{3} = 1.$$

$$\Rightarrow (2+\alpha)^{-1} = \frac{1}{3}\cdot(2-\alpha)$$

Theorem 25 Let K be a field and $g \in K[t]$ be a polynomial of $\deg(g) \geq 1$. Then, for $f \in K[t]$, the coset $[f]_g$ is invertible in $K[t]/g$ if and only if 1 is a greatest common divisor of f and g.

Proof: the greatest common divisor of f and g is a polynomial of the largest degree that divides both f and g. So, the degree d of the greatest common divisor is not larger than the degree of g. Let's consider cases.

Case 1: $d = \deg(g)$. In that case, g is a greatest common divisor of f and g, which means that f is divisible by g.

So, $[f]_g = [0]_g$, which implies that $[f]_g$ is not invertible.

Case 2: $d = 0$. In this case, 1 is a greatest common divisor of f and g. The Extended Euclidean Algorithm gives a representation $1 = a \cdot f + b \cdot g$, where $a, b \in K[t]$.

Consequently, $[1]_g = [a]_g \cdot [f]_g$, which shows that the inverse of $[f]_g$ is $[a]_g$.

Case 3: $0 < d < \deg(g)$. Let p denote a greatest common divisor of f and g. So, $\deg p = d$ and p divides both f and g. Hence, $f = p \cdot h$ and $g = p \cdot q$ for some $h, q \in K[t]$. We consider the product of $[f]_g$ and $[q]_g$:

$$[f]_g \cdot [q]_g = [f \cdot q]_g = [p \cdot h \cdot q]_g = [h \cdot g]_g = [0]_g.$$

Furthermore, $[f]_g \neq [0]_g$, because $d < \deg(g)$ and so f is not divisible by g, and $[q]_g \neq [0]_g$ too,

because $\deg g = \deg p + \deg q$, which implies that $0 < \deg q < \deg g$.

By this, we have shown that $[f]_g$ is a zero divisor. Consequently, by Proposition 4, $[f]_g$ is not invertible. □

Corollary 26 Let K be a field and $g \in K[t]$ be a polynomial with $\deg g \geq 1$. Then $K[t]/g$ is a field if and only if g is irreducible.

Proof: If g is not irreducible, then g is a product $g = p \cdot q$ of polynomials $p, q \in K[t]$ with $\deg p \geq 1$ and $\deg q \geq 1$. Since $\deg g = \deg p + \deg q$, we have $\deg p < \deg g$ and $\deg q < \deg g$. Hence, neither p nor q is dividing by g, which means that $[p]_g \neq [0]_g$ and $[q]_g \neq [0]_g$. On the other hand, $[p]_g \cdot [q]_g = [p \cdot q]_g = [g]_g = [0]_g$. Consequently, $[p]_g$ and $[q]_g$ are

zero divisors in $K[t]/g$. Since, by Proposition 1, zero divisors are not invertible, $K[t]/g$ is not a field.

Conversely, if g is irreducible, then for every $f \in K[t]$ either f is divisible by g and then $[f]_g = [0]_g$ or otherwise 1 is a greatest common divisor of f and g and then, by Theorem 25, $[f]_g$ is invertible in $K[t]/g$. We have shown that every non-zero element of $K[t]/g$ is invertible. Thus, $K[t]/g$ is a field. □

Example $\mathbb{Q}[t]/g$ with $g = t^2 - 2$ is a field. Why?

If g were reducible, we had $g = (t-a)\cdot(t-b)$ with $a, b \in \mathbb{Q}$. Then we would have

$t^2 - (a+b)t + a\cdot b = t^2 - 2$. This implies that $a + b = 0$ and $a \cdot b = -2$. So,

$-2 = a \cdot b = a \cdot (-a) = -a^2$, which gives that $a^2 = 2$ for $a \in \mathbb{Q}$. But such a does not exist ($\sqrt{2}$ is an irrational number, which one can show). This is a contradiction to the existence of the factorization $g = (t-a) \cdot (t-b)$ with $a, b \in \mathbb{Q}$. So, g is irreducible and, by Corollary 26,

$F = \mathbb{Q}[t]/g$ is a field.

Let $\alpha = [t]_g$. Then we know that $\alpha^2 = 2$.

It turns out that every element of F can be written as $x + \alpha y$ with $x, y \in \mathbb{Q}$.

$$\alpha^2 - 2 = [t]_g \cdot [t]_g - [2]_g$$
$$= [t \cdot t - 2]_g = [g]_g = [0]_g$$

$[t^3+t]_g$

$$\begin{array}{r|l} (t^3+t) & t^2-2 = t \\ -\underline{t^3-2t} & \\ 3t & \end{array}$$

$$[t^3+t]_g = [t(t^2-2)+3t]_g = [3t]_g$$

In other words, $\alpha^3+\alpha = 3\alpha$.