Example We consider $F = \mathbb{Q}[t]/g$ where

$g = t^2 - t - 1$ $\quad \alpha := [t]_g \Rightarrow \alpha^2 - \alpha - 1 = 0.$

Let's represent $u = [t^4 - 2t^2]_g$ as $u = x + y\alpha$

where $x, y \in \mathbb{Q}$.

$$t^4 - 2t^2 : (t^2 - t - 1) = t^2 + t$$
$$\underline{t^4 - t^3 - t^2}$$
$$t^3 - t^2$$
$$\underline{t^3 - t^2 - t}$$
$$t$$

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

$$\Rightarrow [t^4 - 2t^2]_g = [t]_g$$

$$\Leftrightarrow \alpha^4 - 2\alpha^2 = \alpha$$

Another way of writing: $\alpha^2 = \alpha + 1$

$$\alpha^4 - 2\alpha^2 = \alpha^2 \cdot \alpha^2 - 2\alpha^2$$
$$= (\alpha+1)\cdot\alpha^2 - 2\alpha^2$$
$$= \alpha^3 - \alpha^2$$
$$= \alpha^2 \cdot \alpha - \alpha^2$$
$$= (\alpha+1)\cdot\alpha - \alpha^2$$
$$= \alpha^2 + \alpha - \alpha^2$$
$$= \alpha$$

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

How do we write α^6 as $x+\alpha y$ with $x, y \in \mathbb{Q}$?

$$\alpha^6 = (\alpha^2)^3 = (\alpha+1)^3 = \alpha^3 + 3\alpha^2 + 3\alpha + 1$$
$$= \alpha^2(\alpha+3) + 3\alpha + 1$$
$$= (\alpha+1)(\alpha+3) + 3\alpha + 1$$
$$= \alpha^2 + 4\alpha + 3 + 3\alpha + 1$$
$$= (\alpha+1) + 4\alpha + 3 + 3\alpha + 1$$
$$= 5 + 8\alpha$$

Vector spaces, linear maps and the dimension

Def A vector space V over a field K (sometimes also called a K-vector space) is a set with two operations

$$+ : V \times V \to V \qquad \text{(vector addition)}$$

$$\cdot : K \times V \to V \qquad \text{(scalar multiplication)}$$

such that:

→ $(V, +)$ is an Abelian group

→
$$(\alpha + \beta) \cdot u = \alpha \cdot u + \beta \cdot u$$
$$\alpha \cdot (u + v) = \alpha \cdot u + \alpha \cdot v$$
$$1 \cdot u = u$$
$$\alpha \cdot (\beta \cdot u) = (\alpha \cdot \beta) \cdot u$$

hold for all $\alpha, \beta \in K$ and all $u, v \in V$.

Remark. For $n \in \mathbb{N}_0$ and any a field K the set

$$K^n = \underbrace{K \times \dots \times K}_{n} \quad \text{with}$$

$$(x_1, \dots, x_n) + (y_1, \dots, y_n) := (x_1 + y_1, \dots, x_n + y_n) \text{ and}$$

$$\alpha \cdot (x_1, \dots, x_n) := (\alpha x_1, \alpha x_2, \dots, \alpha \cdot x_n)$$

for $x = (x_1, \dots, x_n) \in K^n$, $y = (y_1, \dots, y_n) \in K^n$ and $\alpha \in K$

is a vector space over K.

Def Let K be a field and V and W be vector spaces over K.

Then a map $F: V \to W$ is called K-linear (or just linear) if $F(\alpha u + \beta v) = \alpha F(u) + \beta F(v)$

holds for all $\alpha, \beta \in K$ and $u, v \in V$.

Def Let V be a vector space over a field K.

If there exists a bijective K-linear map

$F: K^n \to V$ for $n \in \mathbb{N}_0$, then V is said to be n-dimensional over K.

Remark This n is uniquely determined by V and is called the dimension of V.

Notation: $\dim_K(V)$ or merely $\dim(V)$ if the choice of K is clear from the context.

Proposition 27 Let K be a field and $g \in K[t]$ be a polynomial of degree $n \in \mathbb{N}$. Then $R := K[t]/g$ is a K-vector space of dimension n.

Sketch of the proof:

There is an addition in R, the addition of cosets, and there is a scalar multiplication

$$\alpha \cdot [f]_g := [\alpha f]_g \qquad (\alpha \in K,\ f \in K[t])$$

It's straightforward to see that R is a vector space w.r.t. these two operations.

Let $\omega := [t]_g$. It turns out that the map

$$\varphi : K^n \longrightarrow R \text{ given by}$$

$$\varphi(c_0, \dots, c_{n-1}) := c_0 \cdot \omega^0 + \dots + c_{n-1} \cdot \omega^{n-1}$$

is K-linear and bijective; it's quite straightforward to show this. □

Example Let's construct a finite field with 4 elements.

We take $\mathbb{Z}_2$, the finite field with 2 elements, and construct $F = \mathbb{Z}_2[t]/g$ where $g \in \mathbb{Z}_2[t]$ is an irreducible polynomial of degree 2.

$$\left.\begin{aligned} &t^2 = t \cdot t \\ &t^2 + 1 \\ &t^2 + t = t \cdot (t+1) \\ &t^2 + t + 1 \end{aligned}\right\} \text{ all polynomials of degree 2 in } \mathbb{Z}_2[t]$$

t^2+1 has the zero $t=1$ in $\mathbb{Z}_2$:

$1^2 + 1 = 1 + 1 = 0$ in $\mathbb{Z}_2$

$\Rightarrow t^2 + 1 = (t+1)^2$ in $\mathbb{Z}_2[t]$, why so?

$$(t+1)^2 = (t+1)(t+1) = t^2 + t + t + 1 = t^2 + \underbrace{(1+1)}_{0 \text{ in } \mathbb{Z}_2} \cdot t + 1$$

What about t^2+t+1 ?

It is irreducible. Indeed, if it were reducible then it would be a product of two polynomials of degree one. As polynomials of degree one in $\mathbb{Z}_2[t]$ have a zero in $\mathbb{Z}_2$, t^2+t+1 too would have a zero in $\mathbb{Z}_2$. But it doesn't:

$$0^2 + 0 + 1 = 1 \neq 0$$

$$1^2 + 1 + 1 = 1 + 1 + 1 = 0 + 1 = 1 \neq 0.$$

$\Rightarrow F = \mathbb{Z}_2[t]/g$ with $g = t^2+t+1$ is a field.

Let us denote $[t]_g$ as α. $\alpha := [t]_g$.

$\alpha^2 + \alpha + 1 = 0 \iff \alpha^2 = \alpha + 1$

$\Rightarrow F = \{ \underbrace{0, 1}_{\mathbb{Z}_2}, \alpha, 1+\alpha \}$ and it contains $\mathbb{Z}_2$

F is a two-dimensional vector space over $\mathbb{Z}_2$.

Let's create tables for $+$ and $\cdot$ in F.

$+$	0	1	α	$1+\alpha$
0	0	1	α	$1+\alpha$
1	1	0	$1+\alpha$	α
α	α	$1+\alpha$	0	1
$1+\alpha$	$1+\alpha$	α	1	0

$\cdot$	0	1	α	$1+\alpha$
0	0	0	0	0
1	0	1	α	$1+\alpha$
α	0	α	$1+\alpha$	1
$1+\alpha$	0	$1+\alpha$	1	α

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

Example Let's determine all degree-three irreducible polynomials in $\mathbb{Z}_2[t]$. Let's consider an $f \in \mathbb{Z}_2[t]$ of $\deg f = 3$. When is it irreducible? It turns out that in the case $\deg f = 3$, f is irreducible if and only if f has no zeros in $\mathbb{Z}_2$ (which means, $f(0) \neq 0$ and $f(1) \neq 0$). Indeed, if f has a zero $a \in \mathbb{Z}_2$, then f is divisible by $t-a$ and thus is a product of a degree-one and degree-two polynomial. This shows that such f is reducible.
Conversely, if f is reducible, since $\deg f = 3$, it factors into the product of polynomials of degree 1 and degree 2. The factor of degree one has a zero, which is also a zero of f.

So, our f is reducible if and only if f has a zero in $\mathbb{Z}_2$.
Consequently, f is irreducible if and only if f has no zeros in $\mathbb{Z}_2$.

So, an irreducible f has the form

$$f = t^3 + a \cdot t^2 + b \cdot t + 1$$

($a \in \mathbb{Z}_2$, $b \in \mathbb{Z}_2$, the $+1$ makes sure that $f(0) \neq 0$.)

The condition $f(0) \neq 0$ is guaranteed for this f.
The only choices with $f(1) \neq 0$ are
$a = 1, b = 0$ and $a = 0, b = 1$. So, there are exactly two irreducible polynomials of degree 3 in $\mathbb{Z}_2[t]$:
they are $t^3 + t^2 + 1$ and $t^3 + t + 1$.

Example (follow up on the previous one) We've got two fields with 8 elements each:
$F := \mathbb{Z}_2[t]/f$, where $f := t^3 + t^2 + 1$, and
$G := \mathbb{Z}_2[t]/g$, where $g := t^3 + t + 1$.

Let's determine $f(t+1)$:

$$f(t+1) = (t+1)^3 + (t+1)^2 + 1$$

$$= (t+1)^3 + (t+1)(t+1) + 1$$

$$= (t+1)^3 + t^2 + \underbrace{(1+1)}_{0} \cdot t + 1 + 1$$

$$= (t+1)^3 + t^2 + 1^0 + 1$$

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

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

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

$$= t^3 + t^2 + t + 1 + t^2$$

$$= t^3 + t + 1 = g(t).$$

This means that for the cosets of $\mathbb{Z}_2[t]/f$ and in $\mathbb{Z}_2[t]/g$ there is a natural correspondence: for $h \in \mathbb{Z}_2[t]$ we have

$$[h(t)]_{f(t)} \longleftrightarrow [h(t+1)]_{f(t+1)} = [h(t+1)]_{g(t)}.$$

This correspondence turns out to be a unitary isomorphism. This shows that the fields F and G are essentially the same thing. Let's make this abstract message more explicit.

Let $\alpha := [t]_f$, which means $f(\alpha) = \alpha^3 + \alpha^2 + 1 = 0$

What is $g(\alpha+1)$? We know $f(t+1) = g(t)$.

So $g(\alpha+1) = f((\alpha+1)+1) = f(\alpha) = 0$. So,

$\alpha+1$ is a zero of $g(t) = t^3 + t + 1$.

But in $G = \mathbb{F}_2[t]/g$ one has the coset $\beta := [t]_g$, which satisfies $g(\beta) = \beta^3 + \beta + 1 = 0$.

So, $\alpha+1 \in F \longleftrightarrow \beta \in G$.

Example Let's invert some elements in $\mathbb{Z}_2[t]/g$, where $g = t^3 + t + 1 \in \mathbb{Z}_2[t]$. Let's use $\beta := [t]_g$, which means $\beta^3 + \beta + 1 = 0$.

Let's try to invert $\beta^2 + \beta + 1$. Let's consider the polynomials

$$\begin{cases} f = t^2 + t + 1, & (1) \\ g = t^3 + t + 1. & (2) \end{cases}$$

We run the EEA on the input (f, g).

$$\begin{array}{r} (t^3 + t + 1) : (t^2 + t + 1) = t + 1 \\ t^3 + t^2 + t \\ \hline t^2 + 1 \\ t^2 + t + 1 \\ \hline t \end{array}$$

We multiply (1) with $t+1$ and add the result to (2). This gives:

$$\begin{cases} f = t^2 + t + 1 & (3) \\ (t+1)f + g = t & (4) \end{cases}$$

$(t^2+t+1) : t = t+1$

t^2

$t+1$

t

1

we multiply (4) with $t+1$ and add the result to (3)

$$\begin{cases} t^2 f + (t+1)g = 1 & (5) \\ (t+1)f + g = t & (6) \end{cases}$$

(5) is enough to get the inverse. (5) implies

$$t^2 \cdot f \equiv 1 \pmod{g}.$$

This means $t^2 \cdot (t^2+t+1) \equiv 1 \pmod{g}$,

which means that $\beta^2 \cdot (\beta^2+\beta+1) = 1$

in $\mathbb{Z}_2[t]/q$. So, $(\beta^2+\beta+1)^{-1} = \beta^2$.

Def Two fields F and G are called isomorphic if they are isomorphic as unitary commutative rings;

That means, there exists a unitary isomorphism

$\varphi: F \to G$.

Theorem 28 (The fundamental theorem of finite fields)

the size of every finite field is a power $q = p^n$

of a prime number p (here, $n \in \mathbb{N}$).