9. Finite fields

9.1 Quotients of polynomial rings with coefficients in a finite field

Using the Isomorphism Theorem for Rings, we can reformulate Proposition 7.1.15, which said that a **non-zero** element $a \in \mathbb{Z}_n$ is a unit $\Leftrightarrow \gcd(a,n) = 1$, and is a zero divisor $\Leftrightarrow \gcd(a,n) > 1$:

Proposition 9.1.1: units and zero divisors in $\mathbb{Z}_n$ (p183)

Let $n \in \mathbb{Z}_{>0}, a \in \mathbb{Z}$. Then **exactly one** of the following three cases holds:

1. $a + n\mathbb{Z}$ is the **zero element** in $\mathbb{Z}/n\mathbb{Z}$, equivalently: $\gcd(a,n) = n$,
2. $a + n\mathbb{Z}$ is a **zero-divisor** in $\mathbb{Z}/n\mathbb{Z}$, equivalently: $1 < \gcd(a,n) < n$,
3. $a + n\mathbb{Z}$ is a **unit** in $\mathbb{Z}/n\mathbb{Z}$, equivalently: $\gcd(a,n) = 1$.

A similar proposition holds for quotient rings of polynomial rings with coefficients in a field:

Proposition 9.1.2: units and zero divisors in $\mathbb{F}[X]/(p(x))$ (p184)

Let $(\mathbb{F}, +, \cdot)$ be a field, and suppose that $f(X) \in \mathbb{F}[X]$ is a non-constant polynomial of degree $\boxed{d \geq 1}$. Further let $g(X) \in \mathbb{F}[X]$ be an arbitrary polynomial. Then **exactly one** of the following three cases holds:

1. $g(X) + \langle f(X) \rangle = 0 + \langle f(X) \rangle$, the **zero element** in $\mathbb{F}[X]/\langle f(X) \rangle$.

$$\boxed{\deg(\gcd(g(X), f(X))) = d}$$

2. $g(X) + \langle f(X) \rangle$ is a **zero-divisor** in $\mathbb{F}[X]/\langle f(X) \rangle$.

$$\boxed{0 < \deg(\gcd(g(X), f(X))) < d}$$

3. $g(X) + \langle f(X) \rangle$ is a **unit** in $\mathbb{F}[X]/\langle f(X) \rangle$.

$$\boxed{\deg(\gcd(g(X), f(X))) = 0} \iff \gcd(g(X), f(X)) = 1$$

Facts about the GCD

$$\boxed{m(X) := \gcd(g(X), f(X))} \implies \exists p_1, p_2 \in \mathbb{F}[X] : \begin{cases} \boxed{f(X) = m(X) \cdot p_1(X)} \\ \boxed{g(X) = m(X) \cdot p_2(X)} \end{cases}$$

and from the E.E.A. we know that $\exists r(X), s(X) \in \mathbb{F}[X]$ such that

$$\boxed{m(X) = r(X) \cdot f(X) + s(X) \cdot g(X)}$$

Multiplicative inverse of a unit $g(X) + \langle f(X) \rangle$ in $\mathbb{F}[X]/\langle f(X) \rangle$

From the proof on Blackboard 3, it follows that

$$\begin{aligned} m(X) = 1 &\implies g(X) + \langle f(X) \rangle \text{ is a unit in } \mathbb{F}[X]/\langle f(X) \rangle \\ &\implies \big(g(X) + \langle f(X) \rangle\big)^{-1} = s(X) + \langle f(X) \rangle \end{aligned}$$

So the **multiplicative inverse of a unit** $g(X) + \langle f(X) \rangle$ is given by

$$\boxed{s(X) + \langle f(X) \rangle}$$

where $s(X)$ is obtained from the Extended Euclidean Algorithm such that

$$\boxed{\gcd(f(X), g(X)) = 1 = r(X) \cdot f(X) + s(X) \cdot g(X)}$$

Zero Divisors in Quotient Rings

Given a **proper** factorization $f(X) = f_1(X) \cdot f_2(X)$ of the **reducible polynomial** $f(X)$ where $\deg(f_1), \deg(f_2) < \deg(f)$, then:

$$\boxed{\begin{matrix} \\ f_1(X) + \langle f(X) \rangle \\ \text{and} \quad \text{are ero divisors in } \mathbb{F}[X]/\langle f(X) \rangle \\ f_2(X) + \langle f(X) \rangle \end{matrix}}$$

$$\begin{aligned} \boxed{\big(f_1(X) + \langle f(X) \rangle\big) \cdot \big(f_2(X) + \langle f(X) \rangle\big)} &= f_1(X) \cdot f_2(X) + \langle f(X) \rangle \\ &= f(X) + \langle f(X) \rangle \\ &= \boxed{0 + \langle f(X) \rangle} \end{aligned}$$

Verification of non-zero-ness:
We must ensure neither factor is already zero in the quotient. Suppose for contradiction that $f_1(X) + \langle f(X) \rangle = 0 + \langle f(X) \rangle$. Then $f_1(X) \in \langle f(X) \rangle$, meaning there exists $q(X) \in \mathbb{F}[X]$ such that:

$$f_1(X) = f(X) \cdot q(X)$$

Taking degrees on both sides:

$$\deg(f_1) = \deg(f) + \deg(q)$$

Since $q(X)$ cannot be the zero polynomial, $\deg(q) \geq 0$. This implies $\deg(f_1) \geq \deg(f)$.
However, this contradicts our initial assumption that $f_1(X)$ is a **proper** factor ($\deg(f_1) < \deg(f)$). Thus, $f_1(X) + \langle f(X) \rangle \neq 0$.

Why must f be reducible?
If f is irreducible, it doesn't have zero divisors in $\mathbb{F}[X]/\langle f(X) \rangle$ because all non-zero elements are units (since the quotient group is a field).

Fact

Furthermore, **any non-zero constant multiple** of these proper factors is also a zero divisor.

because

$$g(X) \cdot p_1(X) = m(X) \cdot p_2(X) \cdot p_1(X) = f(X) \cdot p_2(X) \in \langle f(X) \rangle.$$

and for an ideal I, we have that

$$\boxed{i \in I \implies i + I = 0 + I = I}$$

Zero divisor, given another zero divisor

If $g(X) + \langle f(X) \rangle$ is a zero divisor in $\mathbb{F}[X]/\langle f(X) \rangle \iff 0 < \deg(\gcd(g(X), f(X))) < d$, then we can find another zero divisor $v \in \mathbb{F}[X] \setminus \{0_Q\}$ for which $u \cdot v = 0_Q = 0 + \langle f(X) \rangle$, namely

$$\boxed{v(X) = p_1(X) + \langle f(X) \rangle = \frac{f(X)}{\gcd\left(f(X), g(X)\right)} + \langle f(X) \rangle}$$

Why is that? Because

$$\begin{aligned} u(X) \cdot v(X) &= \big(g(X) + \langle f(X) \rangle\big) \cdot \big(p_1(X) + \langle f(X) \rangle\big) \\ &= g(X) \cdot p_1(X) + \langle f(X) \rangle \\ &= m(X) \cdot p_2(X) \cdot p_1(X) + \langle f(X) \rangle \\ &= f(X) \cdot p_2(X) + \langle f(X) \rangle \\ &= 0 + \langle f(X) \rangle \end{aligned}$$

Proper monic factor is a zero divisor

If $f(X) \in \mathbb{F}[X]$ has a **proper monic factor** $h(X) \in \mathbb{F}[X]$, then the coset

$$\boxed{h(X) + \langle f(X) \rangle}$$

is a zero divisor in $\mathbb{F}[X]/\langle f(X) \rangle$.

In this case, $\gcd(f(X), h(X)) = h(X)$, and since $h(X)$ is a proper factor, we have that $0 < \deg(h(X)) < \deg(f(X)) \implies 0 < \deg(\gcd(f(X), h(X))) < \deg(f(X))$, so by Proposition 9.1.2, $h(X) + \langle f(X) \rangle$ is a zero divisor in $\mathbb{F}[X]/\langle f(X) \rangle$.

Furthermore, **any multiple** of this proper monic factor with degree less than $\deg(f(X))$ is also a zero divisor:

Multiple of proper monic factor is a zero divisor

For a proper monic factor $h(X) \in \mathbb{F}[X]$ of $f(X) \in \mathbb{F}[X]$

$$\boxed{h(X) \cdot a(X) + \langle f(X) \rangle \textbf{ is a ero divisor}} \text{ in } \mathbb{F}[X]/\langle f(X) \rangle \text{ if } \boxed{\deg(h(X) \cdot a(X)) < \deg(f(X))}$$

Why is this the case? Because $\gcd(f(X), h(X) \cdot a(X))$ has degree at least $\deg(h(X))$ (since $h(X)$ divides both $f(X)$ and $h(X) \cdot a(X)$), and since $\deg(h(X)) < \deg(f(X))$, we have that

$$0 < \deg(\gcd(f(X), h(X) \cdot a(X))) < \deg(f(X)),$$

so by Proposition 9.1.2, $h(X) \cdot a(X) + \langle f(X) \rangle$ is a zero divisor in $\mathbb{F}[X]/\langle f(X) \rangle$.

Finding zero divisors based on a factorization into irreducible polynomials

Consider the field $\mathbb{F}_p$ with p a prime and let $f(X) \in \mathbb{F}_p[X]$ be a non-constant polynomial with the factorization into k irreducible polynomials (**proper factors**):

$$f(X) = h_1(X) \cdot h_2(X) \cdot \ldots \cdot h_k(X)$$

We find zero divisors in the quotient ring $\mathbb{F}_p[X]/\langle f(X)\rangle$ as follows:

1. Convert each $h_i(X)$ into a **monic** polynomial by multiplying with the inverse of its leading coefficient.
2. **Any proper monic factor $h_i(X)$ gives rise to a zero divisor**

   $$\boxed{h_i(X) + \langle f(X)\rangle}$$

   $\implies$ **already k zero divisors** found.
3. Any **multiple** of $h_i(X)$ with degree less than $\deg(f(X))$ also gives rise to a zero divisor

   $$\boxed{h_i(X) \cdot a(X) + \langle f(X)\rangle}$$

   in $\mathbb{F}_p[X]/\langle f(X)\rangle$.
   - Start with the **constant** multiples of each $h_i(X)$
     - $\deg(h_i(X) \cdot a) = \deg(h_i(X)) < \deg(f(X))$
     - $\implies k \cdot (p-1)$ **extra zero divisors** found.
   - Then consider other **until the degree reaches** $\deg(f(X))$
     - We have $p^{\deg(f(X)) - \deg(h_i(X))}$ polynomials $a(X)$ such that $\deg(h_i(X) \cdot a(X)) < \deg(f(X))$, because each polynomial is uniquely determined by its coefficients.
     - E.g. $h_1(X) \cdot h_2(X)$: $\boxed{\deg(\gcd(f(X), h_1(X) \cdot h_2(X))) = \deg(h_1(X) \cdot h_2(X)) < \deg(f(X))}$ so we can apply Proposition 9.1.2 to conclude that $(h_1(X) \cdot h_2(X)) + \langle f(X)\rangle$ is also a zero divisor.

9.2 Construction of fields using irreducible polynomials

We saw already a field $(\mathbb{Z}_p, +_p, \cdot_p) = (\mathbb{F}_p, +, \cdot)$ can be constructed as the quotient ring $\mathbb{Z}/p\mathbb{Z}$ where p is a prime number.

Another procedure to produce fields is by considering **quotient rings** of $\mathbb{F}[X]$, the polynomial ring with coefficients in a field $\mathbb{F}$. We will need the **analogue of prime numbers for polynomials**, which are called **irreducible polynomials**.

Factors of a polynomial

Let $f(X) \in \mathbb{F}[X]$ be a polynomial. If we can write a **product of factors = factorization**

$$\boxed{f(X) = g(X) \cdot h(X)}$$

for some polynomials $g(X), h(X) \in \mathbb{F}[X]$, then we say that $g(X)$ and $h(X)$ are **factors** of $f(X)$.

We call $g(X)$ a **proper factor** of $f(X)$ if

$$\boxed{0 < \deg(g(X)) < \deg(f(X))}$$

Definition irreducible polynomial (p186)

Let $(\mathbb{F}, +, \cdot)$ be a field. A polynomial $f(X) \in \mathbb{F}[X]$ is called **irreducible** if

$$\boxed{\deg(f(X)) \geq 1 \text{ and } f(X) \text{ has no proper factors}}$$

It is **only divisible by itself or by constant polynomials** (degree 0):

$$\boxed{f(X) = g(X) \cdot h(X) \implies \begin{matrix} \deg(g(X)) = 0 \\ r \\ \deg(h(X)) = 0 \end{matrix}}$$

Definition 9.2.1: irreducible polynomial (p186)

Let $(\mathbb{F}, +, \cdot)$ be a field. A polynomial $f(X) \in \mathbb{F}[X]$ is called **irreducible** if

- it has positive degree: $\deg(f(X)) \geq 1$
- if for $g(X), h(X) \in \mathbb{F}[X]$:

$$\boxed{f(X) = g(X) \cdot h(X) \implies \begin{matrix} \deg(g(X)) = \deg(f(X)) \\ \text{or} \\ \deg(h(X)) = \deg(f(X)) \end{matrix}}$$

BECAUSE RECALL: In a **domain**, $\forall p(X), q(X) \in R[X] : \deg(p(X) \cdot q(X)) = \deg(p(X)) + \deg(q(X))$.
So, in fields (which are $\subseteq$ domains):

$$\boxed{\deg(g(X) \cdot h(X)) = \deg(g(X)) + \deg(h(X))}$$

It is easy to check whether a polynomial of degree at most 3 is irreducible.

Lemma 9.2.4: Irreducibility of 1-degree polynomials (p186)

Let $(\mathbb{F}, +, \cdot)$ be a field. **Any polynomial $f(X) \in \mathbb{F}[X]$ of degree 1 is irreducible**.

Lemma 9.2.5: Irreducibility of 2- and 3-degree polynomials (p186)

Let $(\mathbb{F}, +, \cdot)$ be a field. Let $f(X) \in \mathbb{F}[X]$ be a polynomial with $\deg(f(X)) \in \{2, 3\}$. Then

$$\boxed{f(X) \text{ is irreducible} \iff f(X) \text{ has no roots in } \mathbb{F}}$$

Larger degrees

To find an irreducible polynomial of degree 4 it is **necessary**, **but not sufficient** that the polynomial has no roots!

$$\boxed{f(X) \text{ is irreducible} \implies f(X) \text{ has no roots in } \mathbb{F}}$$

Theorem 9.2.10: Unique factorization into irreducible polynomials

Let $(, +, \cdot)$ be a field. Every polynomial $f(X) \in \mathbb{F}[X]$ of degree at least 1 can be written uniquely as a product of irreducible polynomials, that is, if $p_1(X) \cdot \ldots \cdot p_r(X) = q_1(X) \cdot \ldots \cdot q_s(X)$ where the $p_i(X)$s and the $q_i(X)$'s are irreducible polynomials, then $r = s$ and after relabeling the factors we have $p_i(X) = c_i q_i(X)$ for all i, where the $c_i \in \mathbb{F}$ are nonzero.

In other words, the factorization is **unique up to multiplication by non-zero constants** and rearranging the factors.

Thereom 9.2.12: Construction of fields (p190)

Let $(\mathbb{F}, +, \cdot)$ be a field and let $f(X) \in \mathbb{F}[X]$ be a non-constant polynomial.
Then the quotient ring

$$\boxed{(\mathbb{F}[X]/\langle f(X)\rangle, \cdot, +) \text{ is a } \textbf{field} \iff f(X) \text{ is } \textbf{irreducible}}$$

We can see $\mathbb{F}$ is a subset of $:= \mathbb{F}[X]/\langle f(X)\rangle$ by identifying each element $a \in \mathbb{F}$ with the coset $a + \langle f(X)\rangle \in$.

$$\boxed{\psi : \begin{cases} \mathbb{F} \to \\ a \mapsto a + \langle f(X)\rangle \end{cases} \quad \text{is an injective ring homomorphism}}$$

Notation: extension field (p190)

Let $(\mathbb{F}, +, \cdot)$ be a field and let $f(X) \in \mathbb{F}[X]$ be an **irreducible polynomial**.
Then we define the **extension field**

$$\boxed{:= \mathbb{F}[X]/\langle f(X)\rangle}$$

of $\mathbb{F}$ by $f(X)$. We call $\mathbb{F}$ a **subfield** of .

Lemma 9.2.13 (p190)

Let $f(X) \in \mathbb{F}[X]$ be an irreducible polynomial and define $:= \mathbb{F}[X]/\langle f(X)\rangle$.
Then the element $X + \langle f(X)\rangle \in$ is a root of $f()$ when seen as an element of the set of polynomials []

To avoid confusing elements from with polynomials with coefficients in $\mathbb{F}$, we use the variable when talking about polynomials with coefficients in .
This means that we identify the polynomial

$$a_0 + a_1 X + a_2 X^2 + \ldots + a_n X^n \in \mathbb{F}[X]$$

with the element

$$(a_0 + \langle f(X)\rangle) + (a_1 + \langle f(X)\rangle) + (a_2 + \langle f(X)\rangle)^2 + \ldots + (a_n + \langle f(X)\rangle)^n \in []$$

The above Lemma states that

$$f() = \sum_{i=0}^{d} (a_i + \langle f(X)\rangle)^i \in []$$

has a root at $= X + \langle f(X)\rangle$.

The polynomial

$$f() = \sum_{i=0}^{d} a_i X^i \in \mathbb{F}[X]$$

is identified with the polynomial

$$f() = \sum_{i=0}^{d} (a_i + \langle f(X) \rangle)^i \in []$$

9.3 Construction of finite fields

We will use the notation $\mathbb{F}_q$ for a field with q elements (another common notation is $\mathrm{GF}(q)$, *Galois Field* of order q).

Finite fields have order a prime power

$$\begin{aligned} d &= \deg(f(X)) \geq 1 \\ p &= \text{prime number} \\ q &= p^d \end{aligned}$$

Lemma 9.3.1 (p191): number of elements in quotient ring

Let $f(X) \in \mathbb{F}_p[X]$ be a non-zero polynomial of degree $d \geq 1$. Then the quotient ring

$$\boxed{(\mathbb{F}_p[X]/\langle f(X) \rangle, +, \cdot) \text{ is a finite } \textbf{ring} \text{ with } p^d \text{ elements}}$$

We count the number of elements by considering the standard forms $r(X) + \langle f(X) \rangle$ of the cosets in $\mathbb{F}_p[X]/\langle f(X) \rangle$. For these standard forms, $\deg(r(X)) < d$ or $deg(r(X)) = 0$.

Because the coefficients uniquely determine the polynomial, determining the number of $r(X)$ we can construct is equivalent to choosing the $a_i \in \mathbb{F}_p$ for d coefficients, and thus there are p^d such polynomials.

Theorem 9.3.2 (p192)

Let $f(X) \in \mathbb{F}_p[X]$ be an **irreducible** polynomial of degree d. Then the quotient ring

$$\boxed{(\mathbb{F}_p[X]/\langle f(X) \rangle, +, \cdot) \text{ is a finite } \textbf{field} \text{ with } p^d \text{ elements}}$$

We denote this field by

$$\mathbb{F}_{p^d} = \boxed{\mathbb{F}_q := \left(\mathbb{F}_p[X]/\langle f(X) \rangle, +, \cdot\right)}$$

Number of elements:

$$\boxed{|_q| = q = p^d = |_p[X]/\langle f(X) \rangle|}$$

Fact

$$\mathbb{F}_q = \left(\mathbb{F}_p[X]/\langle f(X) \rangle, +, \cdot\right) \text{ is a } \textbf{field} \iff f(X) \text{ is irreducible}$$

This follows from the fact that by the previous lemma, $|\mathbb{F}_p[X]/\langle f(X) \rangle| = p^d$, and by Theorem 9.2.12, $\mathbb{F}_p[X]/\langle f(X) \rangle$ is a field since $f(X)$ is irreducible.

We will see later that for any prime p and $d \geq 1$, there exists **at least one** irreducible polynomial of degree d in $\mathbb{F}_p[X]$, so finite fields with p^d elements exist for all prime powers.

9.4 Primitive elements in finite fields

We have already seen that the units of a ring $(R, +, \cdot)$ form a group $(R^*, \cdot)$.
In the case of a finite field $(\mathbb{F}_q, +, \cdot)$ where $q = p^d$ for some prime p and $d \geq 1$, we can say more about the structure of the group of units $(\mathbb{F}_q^*, \cdot)$.

Definition: primitive elment

Let $q = p^d$ for some prime p and $d \geq 1$. An element $\in \mathbb{F}_q$ is called a **primitive element** if BOTH

1. $\boxed{\neq 0}$ ($\Leftrightarrow$ $\in \mathbb{F}_q^*$ is a unit)
2. its **multiplicative order** is $\boxed{\text{ord}() = q - 1}$ as an element of the group $(\mathbb{F}_q^*, \cdot)$.

Recall that the order is the smallest positive integer n such that $^n = 1_{\mathbb{F}_q^*}$.

It turns out that the **finite field $\mathbb{F}_q$ ($q = p^d$) always has a primitive element** .
In particular, $(\mathbb{F}_q^*, \cdot)$ is a cyclic group generated by .

Theorem 9.4.1: multiplicative group of finite field is cyclic (p193)

Let $(\mathbb{F}_q, +, \cdot)$ be a finite field with q elements for some prime power $q = p^d$ ($d \geq 1$). Then the multiplicative group of units

$$\boxed{(\mathbb{F}_q^*, \cdot) \text{ is a } \textbf{cyclic} \text{ group}} \qquad \boxed{\mathbb{F}_q^* = \{^0, ^1, ^2, \ldots, ^{q-2}\}}$$

Because in a field $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$, we have that the **order** of this cyclic group is

$$\boxed{|\mathbb{F}_q^*| = q - 1 = \text{ord}()}$$

To prove this, we need to find a generator $\in \mathbb{F}_q^*$ such that any element $h \in \mathbb{F}_q^*$ can be written as $h = ^k$ for some integer $k \geq 0$, which is the **primitive element** of $\mathbb{F}_q$.

Because in a field $\mathbb{F}^* = \mathbb{F} \setminus \{0\}$, we have that

$$\mathbb{F} = \mathbb{F}^* \cup \{0\} \implies \boxed{\mathbb{F} = \{0, ^0, ^1, ^2, \ldots, ^{q-2}\}}$$

By Lemma 3.2.3, we know that a **group of order n is cyclic if and only if it contains an element of order n**. So we need to find an element of order $q - 1$ in $\mathbb{F}_q^*$.

We apply **Lagrange's Theorem** to the group $(\mathbb{F}_q^*, \cdot)$, which says that the order of any subgroup divides the order of the group. Proposition 4.4.4 says that this also holds for $|\langle g \rangle| = \text{ord}(g)$, and thus we have that for any $g \in \mathbb{F}_q^*$

$$\boxed{\text{ord}(g) \mid (q - 1)}$$

Now we can apply Corollory 3.2.6 to this cyclic group of order $q - 1$:

Corollary 9.4.2

Let $(\mathbb{F}_q, +, \cdot)$ be a finite field with q elements for some prime power $q = p^d$ ($d \geq 1$).
Further **let m be a divisor of** $q - 1$. Then

$$\boxed{\text{there exist exactly } \varphi(m) = |\mathbb{Z}_m^*| \text{ elements in } (\mathbb{F}_q^*, \cdot) \text{ with multiplicative order } m}$$

Primitive element (p193)

An element $c \in \mathbb{F}_q^*$ with multiplicative order $q-1$ is called a **primitive element** of the finite field $\mathbb{F}_q$. There exist

$$\boxed{\text{exactly } \varphi(q-1) \text{ primitive elements in } \mathbb{F}_q}$$

So, given a primitive element $c \in \mathbb{F}_q^*$, we can find an $n \in \mathbb{Z}$ such that any element $h \in \mathbb{F}_q^*$ can be written as $h = c^n$, because c is a generator of the cyclic group $\mathbb{F}_q^*$.

Finding a primitive element in $\mathbb{F}_q$

To find a primitive element in $\mathbb{F}_q = \left(\mathbb{F}_p[X]/\langle f(X)\rangle, +, \cdot\right)$ where $f(X) \in \mathbb{F}_p[X]$ is irreducible of degree d ($q = p^d$), we can use the following procedure:

1. Because of Theorem 9.4.1, we know that $(\mathbb{F}_q^*, \cdot)$ is cyclic of order $|\mathbb{F}_q^*| = q-1$.
2. Because of Lagranges Theorem (more specifically Proposition 4.4.4), we know that for any $g \in \mathbb{F}_q^*$

$$\boxed{\text{ord}(g) \text{ divides } (q-1)}$$

3. The possible orders of elements in $\mathbb{F}_q^*$ are the divisors of $q-1$:

$$\boxed{D = \{d \in \mathbb{Z}_{>0} \mid d \text{ divides } (q-1)\}}$$

4. A primitive element is an element $\in \mathbb{F}_q^*$ with order $\text{ord}() = q-1$.
5. We find that primitive element by checking that

$$\text{ord}() = q-1 \iff \boxed{\text{ord}() \notin D \setminus \{q-1\}}$$

In other words, we find an element such that its order is not any of the other divisors of $q-1$.

Factorization of a polynomial over a field

If $f(X) \in \mathbb{F}[X]$ is a polynomial over a field $\mathbb{F}$ with $\deg(f(X)) = d \geq 1$, then we have the following trick to decide if its irreducible or not:

1. Check if it has roots
2. No root $\implies$ cannot be written as a product of degree 1 and degree $d-1$ polynomials
3. Check if it can be factored as a product of two polynomials of degrees a and b where $a, b \geq 2$ and $a + b = d$
   - These two polynomials cannot have roots (else $f(X)$ would have a root)
   - If $a, b \in \{2, 3\}$, the polynomials must be irreducible (else they would have a root)
4. If it cannot be factored in such a way, then it is irreducible.

Exam

To find an irreducible polynomial of degree 5 in $\mathbb{F}_2[X]$, it is sufficient to find a polynomial of degree five that has no factors of degree 1 or 2.

Why?

- If $f(X)$ is reducible into factors $f(X) = g(X) \cdot h(X)$, then $(\deg(g(X)), \deg(h(X))) = (1, 4)$ or $(2, 3)$.
- If $f(X)$ has 3 factors, then $(\deg(g(X)), \deg(h(X)), \deg(k(X))) = (1, 1, 3)$ or $(1, 2, 2)$.
- If $f(X)$ has 4 factors, then $(\deg(g(X)), \deg(h(X)), \deg(k(X)), \deg(l(X))) = (1, 1, 1, 2)$.
- If $f(X)$ has 5 factors, then $(\deg(g(X)), \deg(h(X)), \deg(k(X)), \deg(l(X)), \deg(m(X))) = (1, 1, 1, 1, 1)$.

Finding factors of degree one is equivalent to finding roots.

The only irreducible factors of degree 1 are X and $X+1$, while a direct computation shows that the only irreducible polynomial in $\mathbb{F}_2[X]$ of degree two equals X^2+X+1.