

# Galois Theory - Prerequisites

Pranav Shukla

2026-01-22

## 1 RING THEORY

### Factorization of Polynomials

**Definition** (Irreducible element).

- **In Integral Domains:** Let  $D$  be an integral domain. A polynomial  $f(x)$  from  $D[x]$  which is a non zero and non unit in  $D[x]$  is said to be **irreducible over  $D$**  if  $f(x) = g(x)h(x)$ , where  $g(x)$  and  $h(x)$  are in  $D[x]$  implies that either  $g(x)$  or  $h(x)$  is a unit. A non-zero non unit polynomial in  $D[x]$  is said to be reducible if it is not irreducible over  $D[x]$ .
- **In Fields:** Let  $F$  be a field. Then  $f(x)$ , a non-zero non unit element in  $F[x]$ , is irreducible over  $F$  if there exist  $g(x)$  and  $h(x)$  in  $F[x]$  such that  $f(x) = g(x)h(x)$  implies that  $\deg h(x) < \deg f(x)$  and  $\deg g(x) < \deg f(x)$ .

*Remark.*

- Irreducibility is a property of the polynomial as well as the integral domain or the field being considered.
- One can check that the definition of irreducibility in a field is equivalent to that in an integral domain.

**Definition** (Content of a polynomial, Primitive polynomial).

- **Content of a polynomial:** The content of a polynomial  $a_n x^n + a_{n-1} x^{n-1} + \dots + a_0$  is  $\gcd(a_n, a_{n-1}, \dots, a_0)$ .
- **Primitive polynomial** A primitive polynomial is an element of  $Z[x]$  with content 1.

**Theorem 1** (Reducibility tests for degree 2 and 3).

*Let  $F$  be a field. If  $f(x) \in F[x]$  and  $\deg f(x)$  is 2 or 3, then  $f(x)$  is irreducible over  $F$  iff it has a zero in  $F$ .*

**Theorem 2** (Eisenstein's Criterion 1850).

*Let*

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 \in Z[x]$$

*. If there is a prime  $p$  such that  $p \nmid a_n, p \mid a_i, \dots, p \mid a_0$  and  $p^2 \nmid a_0$ , then  $f(x)$  is irreducible over  $Q$ .*

**Corollary 3** (Irreducibility of  $p$ th Cyclotomic Polynomial).

*For any prime  $p$ , the  $p$ th cyclotomic polynomial*

$$\Phi_p(x) = \frac{x^p - 1}{p - 1} = x^{p-1} + x^{p-2} + \dots + 1$$

*is irreducible over  $Q$ .*

**Theorem 4** ( $\langle p(x) \rangle$  maximal iff  $p(x)$  is irreducible).

*Let  $F$  be a field and let  $p(x) \in F[x]$ . Then  $p(x)$  is irreducible over  $F$  iff  $\langle p(x) \rangle$  is maximal over  $F$ .*

**Corollary 5** ( $F[x]/\langle p(x) \rangle$  is a Field).

*If  $p(x)$  is an irreducible polynomial over  $F$  then  $F[x]/\langle p(x) \rangle$  is a field.*

**Corollary 6** ( $p(x)|a(x)b(x)$  implies  $p(x)|a(x)$  or  $p(x)|b(x)$ ).  
 *$F$  field,  $p(x), a(x), b(x) \in F[x]$  such that  $p(x)|a(x)b(x) \implies p(x)|a(x)$  or  $p(x)|b(x)$*

**Theorem 7** (Unique Factorization in  $\mathbb{Z}[x]$ ).  
*Every non-zero non-unit polynomial in  $\mathbb{Z}[x]$  can be expressed as a product of irreducibles uniquely upto their order and the units.*

## Divisibility in Integral Domains

**Definition** (Associates, Irreducible, Prime).

- Associates: Elements  $a$  and  $b$  in integral domain  $D$  are called associates if we can write  $a = bu$  for some unit  $u$  in  $D$ .
- Irreducible: A non-zero element  $a$  of  $D$  is said to be irreducible over  $D$  if  $b, c \in D$  where  $a = bc$  implies that either  $b$  or  $c$  is a unit.
- Prime: A non-zero element  $p$  is called prime if  $a$  is not a unit and  $p|ab \implies p|a$  or  $p|b$ .

TODO: Norm and its properties

**Theorem 8** (Prime implies Irreducible).  
*In an integral domain, every prime is an irreducible.*

**Theorem 9** (PID implies Irreducible equals Prime).  
*In a principal ideal domain, an element is irreducible if and only if it is a prime.*

**Definition** (Unique Factorization Domain).  
 An integral domain  $D$  is a unique factorization domain if

- every non zero element of  $D$  that is not a unit can be written as a product of irreducibles of  $D$ ; and
- the factorization into irreducibles is unique up to associates and the order in which

the factor appear.

**Lemma 10** (Ascending Chain condition for PID).

*In a principal ideal domain, any strictly increasing chain of ideals  $I_1 \subset I_2 \subset \cdots$  is finite in length.*

**Theorem 11** (PID implies UFD).

*Every principal ideal domain is a unique factorization domain.*

**Corollary 12** ( $F[x]$  is a UFD).

*Let  $F$  be a field. Then  $F[x]$  is a unique factorization domain.*

**Definition** (Euclidean Domain).

An integral domain  $D$  is called an Euclidean domain if there is a function (called the measure) from the nonzero elements of  $D$  to the nonnegative integers such that:

- $d(a) \leq d(ab)$  for all nonzero  $a, b \in D$ ; and
- If  $a, b \in D, b \neq 0$ , then there exist elements  $q$  and  $r$  in  $D$  such that

$$a = bq + r$$

where  $r = 0$  or  $d(r) < d(b)$

**Theorem 13** (ED implies PID).

*Every Euclidean domain is a principal ideal domain.*

**Theorem 14** ( $D$  a UFD implies  $D[x]$  a UFD).

*If  $D$  is a unique factorization domain, then  $D[x]$  is a unique factorization domain.*