Galois Theory - Prerequisites

Pranav Shukla

2026-01-22

Introduction

Hello everyone. I have recently decided to start with Galois Theory in view of my long term goal of studying Algebraic Number Theory. Now maybe I am being a bit desperate here since for Galois Theory one also needs a good understanding of field theory which for me, is a bit rusty at the moment. I have taken a course in introductory abstract algebra at my university in my previous semester (IIIrd sem), which was fairly basic, was taught upto ring theory, also excluding some important portions of group and ring theory. The book that was followed was Gallian. My goal in this post is to revise (and record) the key results, theorems and ideas in ring and field theory especially, which will be of prime importance for starting with Galois Theory. This will be just a collection of theorems and results and I would not include proofs of them here (maybe will add them gradually in the future), as it takes much more time. Also, not having the proofs written down will allow me to try and recall the proof strategy each time I will have to convince myself of the theorem, improving my understanding of the proof in the process.

The Plan

My plan is that for the revision upto field theory, I will be following Gallian. After reaching there, I will switch to Dummit and Foote for the Galois Theory itself. I have also enrolled in the NPTEL course for Galois Theory this sem, which is being taught by Prof. Krishna Hanumanthu and I will be following that course closely too. Pretty excited for what lies ahead!

- Edit: A minor change in the plan. Will be studying field theory mainly from Dummit and Foote. Target day for completion of field theory: **3rd of Febraury**

RING THEORY

Factorization of Polynomials

Definition

Definition 0.0.1.

- **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* $f(x)$ 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

Remark.

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

Definition (Content of a polynomial, Primitive polynomial)

Definition 0.0.2 (Content of a polynomial, Primitive polynomial)**.**

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

Theorem 0.0.1 (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 0.0.2 (Eisenstein's Criterion 1850)**.**

Let

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

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

Note

Corollary 0.0.1 (Irreducibility of pth Cyclotomic Polynomial)**.**
For any prime p, the pth cyclotomic polynomial

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

ir irreducible over Q.

Theorem 0.0.3 ($\langle p(x) \rangle$ 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.

Note

Corollary 0.0.2 (F[x]/<p(x)> is a Field)**.**
If $p(x)$ is an irreducible polynomial over F then $F[x]/\langle p(x) \rangle$ is a field.

Note

Corollary 0.0.3 (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 0.0.4 (Unique Factorization in Z[x])**.**
Every non-zero non-unit polynomial in $Z[x]$ can be expressed as a product of irreducibles uniquely upto their order and the units.

Divisibility in Integral Domains

Definition (Associates, Irreducibe, Prime)

Definition 0.0.1 (Associates, Irreducibe, 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 0.0.1 (Prime implies Irreducible)**.**
In an integral domain, every prime is an irreducible.

Theorem 0.0.2 (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)

Definition 0.0.2 (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 0.0.1 (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 0.0.3 (PID implies UFD)**.**
Every principal ideal domain is a unique factorization domain.

Note

Corollary 0.0.1 (F[x] is a UFD)**.**
Let F be a field. Then $F[x]$ is a unique factorization domain.

Definition (Euclidean Domain)

Definition 0.0.3 (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 0.0.4 (ED implies PID)**.**
Every Euclidean domain is a principal ideal domain.

Theorem 0.0.5 (D a UFD implies D[x] a UFD)**.**
If D is a unique factorization domain, then $D[x]$ is a unique factorization domain.