

# MATH 594 - Finite Fields and Galois Theory

ARessegetes Stery

April 27, 2024

## Contents

<b>1</b>	<b>Review of Ring Theory</b>	<b>2</b>
<b>2</b>	<b>Multiplicity of Root</b>	<b>4</b>
<b>3</b>	<b>Characteristic of a Field</b>	<b>4</b>
<b>4</b>	<b>Algebraic Extensions</b>	<b>6</b>
<b>5</b>	<b>The Splitting Field of a Polynomial</b>	<b>6</b>
<b>6</b>	<b>Separable Extensions</b>	<b>6</b>
<b>7</b>	<b>Normal Extensions</b>	<b>6</b>
<b>8</b>	<b>Galois Extensions</b>	<b>6</b>
<b>9</b>	<b>Algebraic Independence &amp; Transcendence Degree*</b>	<b>6</b>
<b>10</b>	<b>The Fundamental Theorem of Galois Theory</b>	<b>6</b>
<b>11</b>	<b>Norm and Trace Maps</b>	<b>6</b>
<b>12</b>	<b>Solvability by Radicals</b>	<b>6</b>

# 1 Review of Ring Theory

The Galois Theory originates from the question: Given a polynomial with coefficients in a field (e.g.  $\mathbb{Q}$ ), we want to understand the property of its solutions, and the algebraic structure in which the root lies. This section lays some fundamental notions and results for introducing the whole theory.

Setup the convention. All rings have unit element 1; and all ring homomorphisms map 1 to 1. Inclusion maps, in particular, implies that all subrings of a certain ring must include 1.

**Remark 1.1.** An immediate result is that finite domains are fields.

Recall that a ring  $R$  is a domain if and only if zero does not have non-trivial divisors. That is, for all  $x, y \in R \setminus \{0\}$ ,  $xy = 0$ .

For  $a \in R$ ,  $a \neq 0$ , consider the map

$$\varphi : R \rightarrow R \quad x \mapsto ax$$

Since  $R$  is a domain  $\varphi$  maps nonzero elements to nonzero elements, which implies that there exists some  $x_a$  s.t.  $ax_a = 1$ .

This gives an inverse of  $a$ .

**Proposition 1.2.** If  $f : K \rightarrow R$  is a ring homomorphism, and  $K$  is a field. Then  $R \neq \{0\}$  implies that  $f$  is injective.

*Proof.* Recall that the kernel of a particular ring homomorphism is an ideal. Denote  $I = \ker(f) \subseteq K$ . Suppose that  $a \in I$  s.t.  $a$  is nonzero. Then  $a^{-1} \in I$  which gives  $I = (1) = K \implies f(I) = 0$ . But as we require  $f(1) = 1_R \implies 1_R = 0_R$ , i.e.  $R = \{0\}$  which is a contradiction.  $\square$

**Corollary 1.3.** In particular, ring homomorphisms between fields (field extensions)  $K \rightarrow L$  are injective. Not all fields have extensions (ring homomorphisms) between them.

A class of extensions of which we are particularly interested in, is the extension which gives polynomial a root.  $f \in K[x]$  may not have a root; and by extending it  $K[x] \hookrightarrow L[x]$  we may consider roots of  $f \in L[x]$  which may have a root.

**Proposition 1.4.** Let  $k$  be a field, and  $R = k[X]$ . Let  $f \in R \setminus \{0\}$ . Then the followings are equivalent:

- 1)  $f$  is irreducible.
- 2)  $(f)$  is a prime ideal.
- 3)  $(f)$  is a maximal ideal.

*Proof.* Prove the implications cyclically:

- $3) \implies 2)$ . It is a general fact that maximal ideals are prime. Prove the contrapositive: suppose that an ideal  $(f) \subset R$  is not prime, then there exists  $a, b \in R$  s.t.  $ab \in (f)$  and neither  $a$  and  $b$  are in  $(f)$ . Then  $(f) \subset (a) \subset R$  which implies that  $(f)$  is not maximal.
- $2) \implies 1)$ .  $(f)$  being a prime ideal in  $R$  implies that in particular  $(f) \neq R$ , i.e.  $f$  is not invertible. Suppose that there exists  $g, h$  not invertible s.t.  $f = gh$ . Without loss of generality, assume that  $g \in (f)$ . Then there exists some  $u \in R$  s.t.  $g = fu$ . Multiply on the right by  $h$  gives  $f = gh = fuh$  which implies that  $h$  is invertible, giving a contradiction.

- 3)  $\implies$  1).  $f$  being irreducible implies that  $f$  is not invertible, i.e.  $(f) \neq R$ . Suppose that there exists some maximal ideal  $J$  s.t.  $(f) \subset J \subset R$ . Then since maximal ideals are in particular prime,  $J = (g)$  for some  $g \in R$ . But then this implies that  $f = gu$  giving that  $u$  is invertible, and therefore  $(f) = J$ , which is a contradiction.  $\square$

Recall that two elements  $f, g$  are relative prime if for all  $p \in R$  s.t.  $p \mid f, p \mid g$ ,  $p$  is invertible. Then we have the following result similar to the case for integer divisibility:

**Proposition 1.5.** Let  $k$  be a field, and  $R = k[x]$ . For  $f, g, h \in R$  s.t.  $f \mid gh$ , if  $f$  and  $g$  are relative prime, then  $f \mid h$ .

*Proof.* Since  $k$  is a field,  $k[x]$  is a PID (as every element in the coefficient is invertible, for  $a, b$  relative prime  $(a, b) = (1) = k[x]$ ). Consider  $I = (f, g) \subseteq R$ . Since  $I$  is principal,  $I = (p)$  for some  $p \in k[x]$ . Therefore  $p \mid f, p \mid g$ , which implies that  $p$  is invertible. Then  $I = R$ . This gives that there exists  $A, B \in R$  s.t.  $Af + Bg = 1$ . Multiplying  $h$  on the right gives  $Afh + Bgh = h$ . Since  $f$  divides LHS,  $f \mid h$ .  $\square$

**Proposition 1.6.** Let  $k$  be a field, and  $R = k[x]$ . If  $f \in R \setminus \{0\}$ , and denoting  $d = \deg f$ , then there exists field extensions  $k \hookrightarrow L$  and  $a_1, \dots, a_d \in L, c \in k$  s.t.  $f = c(x - a_1) \cdots (x - a_d)$  in  $L[x]$ .

*Proof.* The key step is to show that if  $f$  is irreducible in  $R$ , then there exists a field extension  $k \hookrightarrow k'$  s.t.  $f$  has a root in  $k'$ .

Consider  $k' = k[x]/(f)$ . Since  $f$  is irreducible,  $(f)$  is a maximal ideal in  $R$ , and therefore  $k'$  is a field. Since elements in  $k$  are of degree 0 in  $k[x]$ . Considering  $k \rightarrow k[x] \rightarrow k' := k[x]/(f)$  gives the injective ring homomorphism (field extension). Let  $a = \bar{x} \in k'$ . Then  $f(a) = \overline{f(x)} = 0$ , which implies that  $a$  is a root of  $f$ .

Proceed the rest of the proof by induction:

- $d = 0$ . This is the trivial case.
- $d = 1$ . Then  $f = c(x - a)$  for some  $c, a \in k$ .
- $d \geq 2$ . Apply the above steps iteratively. Then there exists some  $a \in k'$  s.t.  $(x - a) \mid f$ , i.e. in  $k'[x]$  we have the decomposition  $f = (x - a)g$  for some  $g \in k'[x]$  with  $\deg g = \deg f - 1$ . Applying the inductive hypothesis (the results holds in lower degrees) gives the full decomposition in  $L := k'$ .  $\square$

**Notation.** Denote the image of the map  $(k[y] \rightarrow k, y \mapsto a)$  by  $k[a]$ . This is the smallest  $k$ -algebra containing  $a$ .

**Proposition 1.7.** Let  $k$  be a field, and  $R = k[x]$ . Let  $f \in R \setminus \{0\}$  be irreducible. Suppose that we have the field extension  $k \hookrightarrow K$ , and  $a \in K$  is a root of  $f$ . Then  $k[a] \simeq k[x]/(f)$ . In particular,  $k[a]$  is a field.

*Proof.* Consider the ring homomorphism  $\varphi : k[y] \rightarrow K$  s.t.  $\varphi(y) = a$ . Then by the First Isomorphism Theorem, we have  $k[a] = \text{im } \varphi \simeq k[x]/\ker \varphi \simeq k[x]/(f)$  since  $f(a) = 0$ .  $\square$

Notice that every field extension  $k \hookrightarrow K$  is a  $k$ -algebra morphism (ring homomorphisms that are  $k$ -linear). Since  $k$  is a field, this gives  $K$  a  $k$ -vector space structure.

**Definition 1.8 (Degree).** The **degree** of the field extension  $k \hookrightarrow K$  is  $\dim_k K \in \mathbb{Z}_{>0}$  or infinite.

**Definition 1.9 (Finite).** A field extension is **finite** if the degree of it is finite.

**Example 1.10.** If  $f \in k[x]$  is irreducible, and  $K = k[x]/(f)$ , then  $[K : k] = \deg f$ . More generally, if  $g \in k[x]$  is a nonzero polynomial, then  $\dim_k(k[x]/(g)) = \deg g$ .

This can be seen via applying the division algorithm (since  $K[x]$  is an Euclidean Domain. This can be seen via computing the division). Then for all  $P \in k[x]$ , there exists unique  $Q, R \in k[x]$  s.t.  $P = gQ + R$ , with  $\deg R < \deg g$ . Then since  $\bar{P} = \bar{R}$  in  $k[x]/(g)$ ,  $\{\bar{1}, \bar{x}, \dots, \bar{x}^{\deg g - 1}\}$  gives a basis of  $k[x]/(g)$  over  $k$ .

## 2 Multiplicity of Root

This section provides tools for describing the zeros of a polynomial, and how they in general can look like. The proposition below says that any polynomial can be factored into two parts, with the first part having roots in the field; and the second part requires extension of the field to decompose completely.

**Definition 2.1 (Multiplicity).** Let  $f \in k[x]$  be a nonzero polynomial for  $k$  a field, and  $a \in R$  a root of  $f$ , Then  $a$  has **multiplicity**  $m$  if  $(x - a)^m \mid f$ , but  $(x - a)^{m+1} \nmid f$ .

**Proposition 2.2.** If  $f \in R \setminus \{0\}$ , and  $a_1, \dots, a_r \in k$  are pairwise distinct roots of  $f$  s.t.  $a_i$  has multiplicity  $m_i$ . Then we have the decomposition of  $f$ :

$$f = \prod_{i=1}^r (x - a_i)^{m_i} g, \quad g \in R, g(a_i) \neq 0 \text{ for all } i$$

In particular,  $\sum_i m_i \leq \deg f$ .

*Proof.* Apply induction on  $r$ :

- *Base case.* Then  $m_1$  is the maximal integer satisfying the condition that  $(x - a_1)^{m_1} \mid f$ . Then define  $g$  be such that  $f = (x - a_1)^{m_1} g$ .
- *Inductive step.* For  $r \geq 2$ , denote  $f_1$  be the polynomial s.t.  $f = (x - a_1)^{m_1} f_1$ . Notice that for all  $i$  s.t.  $2 \leq i \leq r$ , we have  $(x - a_i)^{m_i} \mid f$ . Then since  $(x - a_i)$  and  $(x - a_1)$  are relative prime (they are both irreducible) by Proposition 1.5 we have  $(x - a_i)^{m_i} \mid f_1$ . Then applying inductive hypothesis gives the desired decomposition of  $f$ .

□

## 3 Characteristic of a Field

Recall that in the first section we mentioned that there does not necessarily exist ring homomorphisms between arbitrary fields. This, as we will see in the following, implies some constraints on the structure that a field can have.

Let  $S$  be an integral domain. Let  $\varphi : \mathbb{Z} \rightarrow S$  s.t.  $n \mapsto n \cdot 1_S$ . This is the unique ring homomorphism between  $\mathbb{Z}$  and  $S$  due to the constraint the 1 should be mapped to 1. Since  $S$  is a domain, and  $\mathbb{Z}$  is a PID,  $\ker \varphi = (d)$  for  $d$  prime or zero. Then either

- 1)  $\ker \varphi = \{0\}$ ; or
- 2)  $\ker \varphi = p\mathbb{Z}$  for some  $p$  prime.

In case 1), if we suppose further that  $S = k$  which is a field, then for all  $n \in \mathbb{Z}$   $\varphi(n)$  is invertible. By the universal property of the quotient ring, this induces a ring homomorphism (which is also a field extension)  $\text{Frac}(\mathbb{Z}) = \mathbb{Q} \hookrightarrow S$ .

In case 2), we have an injective ring homomorphism  $\mathbb{Z}/p\mathbb{Z} \hookrightarrow S$  for some  $p$  prime. Defining  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ,  $S$  becomes an  $\mathbb{F}_p$ -algebra by the  $\varphi$  above.

**Definition 3.1 (Characteristic).** For a field  $k$ , the **characteristic** of  $k$  is

$$\text{char}(k) = \begin{cases} p, & \text{if } \mathbb{F}_p \hookrightarrow k \text{ (case 1)} \\ 0, & \text{if } \mathbb{Q} \hookrightarrow k \text{ (case 2)} \end{cases}$$

**Remark 3.2.** If  $S$  is an  $\mathbb{F}_p$ -algebra (case 2), the map  $F : S \rightarrow S, u \mapsto u^p$  is the Frobenius homomorphism. Check that this is indeed a ring homomorphism:

- $F(uv) = F(u)F(v)$ . Clear as field is commutative:  $(uv)^p = u^p v^p$ .
- $F(u + v) = F(u) + F(v)$ . Compute:

$$(u + v)^p = u^p + v^p + \underbrace{\sum_{i=1}^{p-1} \binom{p}{i} u^{p-i} v^i}_{\text{divisible by } p}$$

where the last term vanishes, as  $\mathbb{F}_p \hookrightarrow S$  should map 0 to 0; and  $\bar{p} = \bar{0} \in \mathbb{F}_p$ .

**4 Algebraic Extensions****5 The Splitting Field of a Polynomial****6 Separable Extensions****7 Normal Extensions****8 Galois Extensions****9 Algebraic Independence & Transcendence Degree\*****10 The Fundamental Theorem of Galois Theory****11 Norm and Trace Maps****12 Solvability by Radicals**