MATH 594 - Finite Fields and Galois Theory

AResseges Stery

April 27, 2024

Contents

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
>
> $$\varphi : R \to R \qquad x \mapsto ax$$
>
> Since R is a domain φ 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 $f : K \to R$ 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 requre $f(1) = 1_R \implies 1_R = 0_R$, i.e. $R = \{0\}$ which is a contradiction. □

> **Corollary 1.3.** In particular, ring homomorphisms between fields (field extensions) $K \to L$ 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.

Notation. A field extension $k \hookrightarrow K$ is also denoted as K/k. These two notations will be used interchangeably.

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.

□

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, $f \mid h$. □

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 $a_1, \ldots, a_d \in L, c \in k$ 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 $k \longrightarrow k[x] \longrightarrow k' := k[x]/(f)$ gives the injective ring homomorphism (field extension). Let $a = \overline{x} \in k'$. 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 $L := k'$.

□

Notation. Denote the image of the map $(k[y] \to k, y \mapsto a)$ 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 $\varphi : k[y] \to K$ s.t. $\varphi(y) = a$. Then by the First Isomorphism Theorem, we have $k[a] = \operatorname{im} \varphi \simeq k[x]/\ker \varphi \simeq k[x]/(f)$ since $f(a) = 0$. □

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 $k \hookrightarrow K$, denoted $[K : k]$, is $\dim_k K \in \mathbb{Z}_{\geq 0}$ or infinite.

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

Remark 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 $\overline{P} = \overline{R}$ in $k[x]/(g)$, $\{\bar{1}, \bar{x}, \ldots, \overline{x^{\deg g - 1}}\}$ 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 $a_1, \ldots, a_r \in k$ are pairwise distinct roots of f s.t. a_i has multiplicity m_i. Then we have the decomposition of f:

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

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 $\varphi : \mathbb{Z} \to S$ 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) $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q} \hookrightarrow S$.

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 φ above.

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

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

Remark 3.2. If S is an $\mathbb{F}_p$-algebra (case 2), the map $F : S \to S$, $u \mapsto u^p$ 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

The field extensions originating solely from "including the roots of polynomials" are the nice ones and deserve a better name. The discussions formalizes the concept of "algebraic closure" in elementary discussions of polynomials.

Proposition 4.1. If $k \hookrightarrow K \hookrightarrow L$ is a field extension, then $[L : k] = [L : K][K : k]$.

Proof. First consider the cases where one of the degrees is infinite:

- If $[K : k]$ is infinite, then $[L : k]$ is infinite as $K \subseteq L$ is a K-vector subspace of L.
- If $[L : K]$ is infinite, then there exists an infinite set of elements which are linearly independent over K, which are also linearly independent over k since $k \subseteq K$.

Now consider the case where both $[L:K]$ and $[K:k]$ are finite. Denote $m=[L:K]$ and $n=[K:k]$. Denote $\{a_1,\dots,a_m\}$ be a basis of L over K, and $\{b_1,\dots,b_n\}$ be a basis of K over k. Notice that $\{a_ib_j \mid 1\le i\le m, 1\le j\le n\}$ gives a basis for L over k, as for all $u\in L$, there exists $\lambda_i\in K$, and thus $\mu_{ij}\in k$ s.t.

$$u=\sum_{i=1}^{n}\lambda_i b_i=\sum_{i,j}\mu_{ij}a_jb_i,\qquad \text{for } \lambda_i=\sum_j \mu_{ij}a_j\mu_{ij}$$

which is a decomposition. They are further linearly independent, as for $u=0$, since b_is give a basis, $\lambda_i=0$ for all i, and therefore $\mu_{ij}=0$ for all i and j. □

Notation. Let $k\hookrightarrow K$ bea field extension, and $A\subseteq K$ a subset. Then we denote

$$k(A):=\cap_{A\subseteq k'}\{k' \mid k\hookrightarrow k'\hookrightarrow K \text{ extension}\}$$

which is the smallest field sub-extension of k inside K containing A.

Remark 4.2. It is worth mentioning that this is different from $k[A]$ which is the smallest k-*subalgebra* containing A:

- They are related via $k(A)=\mathrm{Frac}(k[A])$. They are equal in some "nice" extensions (see Remark 4.9 below).

  By definition we have $k[A]\subseteq k(A)$, as $k[A]$ is only required to be a k-algebra instead of a field extension of k (as field extending k can be seen as k-vector spaces, which are in particular k-algebras). By the universal property of fraction fields, we have $\mathrm{Frac}(k[A])\subseteq k(A)$, as ring homomorphisms between fields are injective, and by definition for all $f\in k[A]$, f has an inverse in $k(A)$. Further since $A\subseteq \mathrm{Frac}(k[A])$ (also by definition, we have $k(A)=\mathrm{Frac}k[A]$).

- Considering multiple elements, we can extend the previous notation, by considering for $A=\{a_1,\dots,a_n\}$, then $k[A]=\mathrm{im}\,\varphi$ for

  $$\varphi: k[x_1,\dots,x_n]\to K,\qquad x_i\mapsto a_i$$

Definition 4.3 (Finite Generated). A field extension K/k is **finitely generated** if there exists $a_1,\dots,a_n\in K$ s.t. $k(a_1,\dots,a_n)=K$.

Remark 4.4. If a field extension K/k is finite, then it is also finitely generated, as K/k being finite implies that there exists some finite basis of K over k; and picking one gives the elements that "finitely generates" K. However, the converse is not true: consider $k\hookrightarrow k(x)=\mathrm{Frac}(k[x])$ is finitely generated (by x) but is not finite (we have the infinite set $\{x^i \mid i\in\mathbb{Z}\}$ whose elements are linearly independent over k)

Definition 4.5 (Algebraic; Transcendental). Let $k\hookrightarrow K$ be a field extension. An element $a\in K$ is **algebraic over** k if there exists $f\in k[x]\setminus\{0\}$ s.t. $f(a)=0$ in $K[x]$. Otherwise a is **transcendental**. An extension K/k is **algebraic** if for all $a\in K$, it is algebraic over k.

Remark 4.6. Consider the field extensions $k\hookrightarrow K\hookrightarrow L$. Then if $a\in L$ is algebraic over k, then a is also algebraic over K, as a algebraic over k implies that there exists $f\in k[x]$ s.t. $f(a)=0$; and by definition we also have $f\in K[x]$.

Remark 4.7. Given a field extension $k \hookrightarrow K$, and $a \in K$. Then a is algebraic if and only if the $\varphi : k[x] \to k, x \mapsto a$ has a non-trivial kernel. This is the direct translation of having a polynomial f with a as its root. Then $\ker \varphi$ is a prime ideal.

To prove this, it suffices to show that $k[x]/(\ker \varphi)$ is a domain. This is indeed the case, as $k[x]$ is a domain: for all $g, h \in k[x]$, $g(a) \neq 0$ and $h(a) \neq 0$ implies that $gh(a) \neq 0$, i.e. $gh \notin \ker \varphi$ ($gh \neq \bar{0}$ in $k[x]/(\ker \varphi)$). Therefore, there exists some f s.t. $\ker \varphi = (f)$.

Definition 4.8 (Minimal Polynomial). $f \in k[x]$ is the **minimal polynomial** of $a \in K$ if for $\varphi : k[x] \to K$, $x \mapsto a$, $\ker \varphi = (f)$. This is well-defined by the above Remark (Remark 4.7).

Remark 4.9. For a being algebraic, f is a maximal ideal (by the fact that $k[x]/(\ker \varphi)$ is a domain). Then $k[a] = k[x]/(\ker \varphi)$ is a field. This gives $k[a] = k(a)$.

Remark 4.10. Given field extension K/k, if $a \in K$ is transcendental over k, then $k[a] \simeq k[x]$, as since there is no polynomial with root a implies that $k[a]$ can be seen as injecting a formal variable to the field $k[x]$. This further implies $k(a) \simeq k(x)$ (as $k(a) \simeq \mathrm{Frac}(k[a])$; and same for x).

Example 4.11. Suppose that $d \in \mathbb{Z}$ is not a square, and let $a = \sqrt{d}$. Consider the field extension $\mathbb{Q} \to \mathbb{C}$.

Since a is not in $\mathbb{Q}$, a cannot be a root of degree 1 polynomials, i.e. the minimal polynomial of a must be of degree at least 2; and we have a as a root of $x^2 - d = 0$, the minimal polynomial of a over k is $x^2 - d = 0$, which also implies that a is algebraic over $\mathbb{Q}$.

Therefore, $\mathbb{Q}(\sqrt{d})$ can be seen as a $\mathbb{Q}$-vector space, which has a basis $\{1, \sqrt{Q}\}$, i.e. $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$. In particular we have $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{d}) = 2$ as $\deg f = 2$, resulting from Remark 1.10.

Proposition 4.12. Every finite extension K/k is algebraic.

Proof. Denote $[K : k] = n$ which is finite. Regarding K as a k-vector space, for all $a \in K$ the set of elements $\{1, a, \ldots, a^n\}$ are linearly dependent (as there are $(n+1)$ of them). That is, there exists $c_0, \ldots, c_n \in k$ s.t. $c_0 + c_1 a + \cdots + c_n a^n = 0$; and $f = c_0 + c_1 x + \cdots + c_n x^n \in k[x] \setminus \{0\}$. This gives a polynomial $f \in k[x]$ s.t. $f(a) = 0$, i.e. a is algebraic. Since $a \in K$ can be taken arbitrarily, we have K/k being algebraic. □

Proposition 4.13. Let $k \hookrightarrow K$ be a field extension, and $a_1, \ldots, a_n \in K$ are algebraic over k. Then $k[a_1, \ldots, a_n] = k(a_1, \ldots, a_n)$; and $k(a_1, \ldots, a_n)$ is a finite extension over k.

Proof. Remark 4.9 gives the case for $n = 1$ $k[a] = k(a)$, and Remark 1.10 (using minimal polynomial) gives that the extension is finite.

For $n \geq 2$, repeat the argument with the induction hypothesis. First by definition we have $k[a_1, \ldots, a_n] = (k[a_1, \ldots, a_{n-1}])[a_n]$; and the same holds for the field extension version (replace brackets with parentheses). Further finite extensions are transitive, by Proposition 4.1. Suppose now that $k' = k[a_1, \ldots, a_{n-1}] = k(a_1, \ldots, a_{n-1})$ is a finite extension over k. Then $k[a_1, \ldots, a_n] = k'[a_n] = k'(a_n) = k(a_1, \ldots, a_n)$ is finite over k'; and by hypothesis we know $k'[a_n]$ is finite over k since k' is. □

Corollary 4.14. Finitely generated algebraic field extensions are finite.

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