Field Extensions and Category Theory

Brian Jiang

In these notes I discuss algebraic field extensions (splitting and separable fields) and category theory, which correspond to sections 1.1 and 1.4 of Szamuely, respectively.

1 Splitting Fields

The notion of splitting fields is motivated by the factorization of polynomials. More specifically,

Definition 1. For field F and nonconstant polynomial $p(x)$, an extension E of F is a splitting field if the roots $\alpha_1, \ldots, \alpha_n$ of $p(x)$ exists in E such that $E = F(\alpha_1, \ldots, \alpha_n)$.

Example 2. Some simple examples.

(i) $\mathbb{Q}(\sqrt{2}, i)$ is a splitting field of $x^4 + 2x^2 - 8$

(ii) $\mathbb{Q}(\sqrt[3]{3})$ is not a splitting field of $x^3 - 3$ due to imaginary roots.

Proposition 3. For any nonconstant polynomial $p(x) \in F[x]$, a splitting field E exists.

Proof. This can be shown using mathematical induction on the order of the polynomial. The important idea is that any non constant polynomial $p(x) \in F[x]$ with order p contains a root α_1 in the field $\frac{F[x]}{<p(x)>}$. Thus we can factor the polynomial into $p(x) = (x - \alpha_1)q(x)$, where $q(x)$ is of order one less than p. ☺

Now consider an isomorphism of fields $\phi: E \to F$, with K the extension field of E with $\alpha \in K$ algebraic over E with minimal polynomial $p(x)$. Let L extend F with algebraic β over $p(x)$ under the image of ϕ. Then we have a unique isomorphism $\bar{\phi} : E(\alpha) \to F(\beta)$ with $\bar{\phi}(\alpha) = \beta$ and $\bar{\phi}$ agrees with ϕ on E. This isomorphism maps an element of $E(\alpha)$, which can be written as $a_0 + \ldots + a_{n-1}\alpha^{n-1}$ to $\phi(a_0) + \ldots + \phi(a_{n-1})\beta^{n-1}$. And thus by induction, we can show that:

Proposition 4. We can find an isomorphism between two splitting fields of F of $p(x)$ that preserves F.

2 Separable Fields

Let $\bar{k}$ denote the algebraic closure of field k. Recall separability intuitively is related to the multiplicity of roots. More specifically,

Definition 5. For field extension $L|K$, $\alpha \in L$ is separable over K if the minimal polynomial, when factored over $\bar{L}$, has no repeated roots. If every $\alpha \in L$ is separable, then $L|K$ is a separable extension.

Lemma 6. For finite field extension $L|k$ of degree n, L has at most n distinct k-algebra homomorphisms to $\bar{k}$, with equality iff $L|k$ is separable.

Proof. Recall in the simplest case where $F = k(\alpha_1)$ that a k-algebra homomorphism $\phi : F \to \bar{k}$, maps $\phi(x) \to x$ for all $x \in k$, and thus is solely defined by where α_1 maps to. And then we proceed by induction on the number of elements that generate L. For example, if there are two elements $F = k(\alpha_1, \alpha_2)$, then we have $[F : k] = [F : k(\alpha_1)][k(\alpha_1) : k]$. And thus α_2 can map to p elements, and α_1 can map to q elements, with $pq = n$. ☺

From this, we easily conclude that for a tower of finite field extensions $L|M|k$, $L|k$ is separable iff $L|M$ and $M|k$ are separable. And thus we see that the compositum is also separable. The compositum of all separable subextensions of $\bar{k}$ is a separable extension, which we call the separable closure.

The multiple roots of polynomial $f \in F[x]$ coincide with the common roots of it's derivative f'. For example, if f contains some multiple root $(x-a)^n, n > 1$ its derivative will also contain some factor of $(x - a)$. If f is irreducible, than it has multiple roots iff $f' = 0$.

Example 7. Fields are perfect if all finite extensions are separable, or if in other words the algebraic and separable closures are the same. Some examples of perfect fields include

(i) Fields of characteristic 0. For any irreducible polynomial $x^n + ... + a_0 \in F[x]$, its gcd with its derivative $nx^{n-1} + ... + a_1$ is 1 (because it is irreducible and characteristic 0).

(ii) Finite fields. Let $\mathbb{F}_p = \mathbb{Z}/\mathbb{Z}_p$ for prime p. All finite fields look like $\mathbb{F}_q = \mathbb{F}_p(x^q - x)$ where $q = p^n$. $\mathbb{F}_q$ however is separable. This is because, $\gcd(x^q - x, qx^q - 1) = \gcd(x^q - x, -1) = 1$. (Note that all elements $a \in \mathbb{F}_p$ satisfy $a^q - a = 0$).

What fields are not separable? Consider the extension $\mathbb{F}_p(t)[x]|(x^p - t)$ is over $\mathbb{F}_p$. The derivative $x^p - t$ is px^{p-1} is zero, so the extension is not separable. Another way to see this is that $x^p - t = (x - t^{1/p})^p$ in $\mathbb{F}_p$.

3 Category Theory: Definitions and Examples

Definition 8. A category C consists of objects and morphisms between the objects. For any two objects A and B, the morphisms $\phi : A \to B$ form a set denoted by $Hom(A, B)$ with the following properties:

(i) $id_A \in Hom(A, A)$, i.e there exists an identity morphism for all objects

(ii) Given two morphisms $\phi \in Hom(A, B)$ and $\psi \in Hom(B, C)$, there exists a composition of morphisms that is associative and preserves the identity ($\phi \circ id_A = \phi$)

Definition 9. A morphism $\phi \in Hom(A, B)$ is an isomorphism if there exists some morphism $\psi \in Hom(B, A)$ such that $\phi \circ \psi = id_B$ and $\psi \circ \phi = id_A$

Example 10. A couple straightfoward example of categories include

(i) Category of sets: objects are sets, morphisms are bijective maps

(ii) Category of groups: objects are groups, morphisms are homomorphisms

(iii) Category of topological spaces: objects are topologies, morphisms are continuous maps

Additionally, for every category C, we have the opposite category C^{op}, which simply reverses the direction of the morphisms: there is a bijection between the sets $Hom(A, B)$ of C and the sets $Hom(B, A)$ of C^{op}

Definition 11. Let ϕ be a morphism from A to B. ϕ is a monomorphism if for any object X and any two morphisms α and α' from X to A, $\phi \circ \alpha = \phi \circ \alpha'$ means $\alpha = \alpha'$. ϕ is an epimorphism of for two morphisms β and β', $\beta \circ \phi = \beta' \circ \phi$ means $\beta = \beta'$.

Example 12. In the category of sets, monomorphisms are one-to-one functions, and epimorphisms are onto functions.

4 Functors

Functors establish relationships between categories

Definition 13. A functor F between two categories C_1 and C_2 consists of:

(i) A map on objects, $A \mapsto F(A)$

(ii) A map on sets of morphisms, $Hom(A, B) \mapsto Hom(F(A), B(A))$ that preserves composition and maps the identity to the identity.

We say that C_1 is the domain and C_2 is the target.

Example 14. We have the identity functor id_C on a category C leaves all morphisms and objects fixed. An example that is little more exciting is the functor π_1 from (pointed) topologies to groups. Specifically, for π maps pointed topologies (X, x_0) to the fundamental group $\pi_1(X, x_0)$.

Recall in the first class we showed that the algebraic closure of $\mathbb{R}$ is C. This required some composition of maps $S^1_r \to \mathbb{C} \to \mathbb{C} - \{0\} \to S^1$. We then applied the functor π_1 to get $\pi_1(S^1_r) \to \pi_1(\mathbb{C}) \to \pi_1(\mathbb{C} - \{0\}) \to \pi_1(S^1)$. Doing this makes sense because maps between these groups also change via the application of the functor.

Example 15. We can consider a category of functors between categories C_1 and C_2. The objects are functors. For functors F and G we have morphisms $\Phi: F \to G$. These morphisms are defined as a set of morphisms inside C_2, $\Phi_A: F(A) \to G(A)$, where A is an object of C_1. For this map to be well defined, for every $\phi: A \to B$ in C_1, we need a commutation relation where $G(\phi) \circ \Phi_A = \Phi_B \circ F(\phi)$. The morphism Φ is an isomorphism if each Φ_A is an isomorphism.

Just as we have an identity morphism, we also have an identity functor. Similarly, just as we have an isomorphism of objects, we have isomophisms of categories.

Definition 16. Two categories C_1 and C_2 are isomorphic if there are two functors $F : C_1 \to C_2$ and $G : C_2 \to C_1$ such that $F \circ G = id_{C_2}$ and $G \circ F = id_{C_1}$. If we merely have an isomorphism of functors with the identity (i.e. there exists an isomorphism of functors Φ such that $\Phi : F \circ G \to id_{C_2}$ and vice-versa), we say that C_1 and C_2 are equivalent.

Example 17. Another example of a functor fixing an object A in category C. We then have a functor $Hom(A,)$ to sets: objects B get mapped to the set $Hom(A, B)$, and morphisms $B \to C$ get mapped to $Hom(A, B) \to Hom(A, C)$.

Definition 18. A functor F from some category C to Sets is representable if there is an object $A \in C$ and an isomophism of functors $F \cong Hom(A,)$,

Lemma 19. If F and G are functors $C \to Sets$ represented by objects A and B, respectively, every morphism of functors $\Phi : F \to G$ of functors is induced by a unique morphism $B \to A$ as above. This statement is Yoneda's lemma.

Proof. Basically we want to show there is an isomorphism from $Hom(Hom(A,), Hom(B,))$ to $Hom(A, B)$. In the forward direction, we can consider a morphism Φ, which contains some morphism $\Phi_A : Hom(A, A) \to \mathrm{Hom}(B, A)$, which maps the identity morphism to some map f. Thus we have a morphism $\Phi \to f$. In the other direction, for any morphism $\phi \in Hom(B, A)$ (or in other words $\phi : B \to A$), we want a mapping that brings a morphism $\psi \in Hom(A, C)$, to some element of $Hom(B, C)$. We do this by mapping ψ to $\psi \circ \phi$. So we have morphisms in both directions, the trick is to show (which I will instead just believe) that these morphisms are isomorphisms. ☺