FIELDS

PRESTON WAKE

1. Introduction

We discuss some basic definitions and properties of fields, culminating with Galois theory.

Definition 1.1. A *field* is a commutative ring in which every non-zero element has a multiplicative inverse.

Definition 1.2. The *characteristic* of a field F, $char(F)$, is the smallest natural number n such that $n \cdot 1 = 0$ in F. If no such number exists, we say $char(F) = 0$.

Exercise 1.3. Show that if $char(F)$ is non-zero, then it is a prime number. Show that if $char(F) = 0$, then F contains a field isomorphic to $\mathbb{Q}$, and if $char(F) = p$, then F contains a field isomorphic to $\mathbb{Z}/p\mathbb{Z}$. This is sometimes called the *prime field* of F.

Note that a field has no non-trivial ideals, since any non-zero ideal must contain a unit. Since the kernal of a ring-map is an ideal, we see that any non-zero ring map out of a field is injective.

2. Examples of Fields

We first discuss two ways to construct a field from a ring.

Exercise 2.1. Show that if R is a commutative ring, and m is a maximal ideal, then R/m is a field.

An an example of this is $\mathbb{Z}/p\mathbb{Z}$. Since this field is finite, it's also often denoted by $\mathbb{F}_p$.

Definition 2.2. Given an integral domain R, we construct the *field of fractions*, $k(R)$, of R as follows: $k(R) = R \times R$ with multiplication $(a, b)(c, d) = (ac, bd)$ and addition $(a, b) + (c, d) = (ad + bc, bd)$. For obvious reasons we denote elements of $k(R)$ by $(a, b) = a/b$.

The obvious example is the rational numbers, $\mathbb{Q} = k(\mathbb{Z})$. For a more interesting example, let Ω be an open set in $\mathbb{C}$ and let $H(\Omega)$ be the ring of holomorphic functions. Then, the field of meromorphic functions, $M(\Omega)$, is $M(\Omega) = k(H(\Omega))$.

Another way to construct new fields is from old fields.

Definition 2.3. If E and F are fields and $F \subset E$, then we say E is an *extension* of F, and sometimes write this information as E/F. We say an element α of E is *algebraic over* F if there is a polynomial f in $F[x]$ such that $f(\alpha) = 0$. We say E is an *algebraic extension* if every element of E is algebraic over F.

Note that an extension E has the structure of F-vector space and F-algebra. The dimension of this vector space is called the *degree* of the extension, and is denoted by $[E : F] = dim_F(E)$. An extension is called *finite* if the degree is finite, and *infinite* otherwise.

Exercise 2.4. Show that any finite extension is algebraic.

Exercise 2.5. Show that if $\alpha \in E$ is algebraic, then there exists a unique monic, irreducible polynomial $min_\alpha(x) \in F[x]$ with α as a root.

An example of a field extension is $\mathbb{R} \subset \mathbb{C}$. Since $\mathbb{C}$ is a 2-dimensional real vector space, it's algebraic (by the exercise). We can show this explicitly: if $\alpha = a+bi \in \mathbb{C}$, then α satisfies $(x-a)^2 + b^2$.

Theorem 2.6. *If E/F is an extension and $\alpha \in E$ is algebraic, then there exists a smallest field, $F(\alpha)$, containing both α and F. The map $\phi : F[x]/(min_\alpha(x)) \to F(\alpha)$ given by $\phi(x) = \alpha$ is an isomorphism.*

The process described in the theorem is called *adjoining α to F*.

Exercise 2.7. Show that the field $\mathbb{Q}(\sqrt{2}, \sqrt{3}, ..., \sqrt{p}, ...)$ obtained by adjoining the square roots of all the prime numbers is an algebraic, but not a finite, extension of $\mathbb{Q}$.

Exercise 2.8. Show that the field of rational functions, $F(x) = k(F[x])$, is a non-algebraic extension of F.

If f is an irreducible polynomial in $\mathbb{F}_p$ of degree n, then $\mathbb{F}_p[x]/(f)$ is a field with $q = p^n$ elements; such a field is denoted by $\mathbb{F}_q$.

Exercise 2.9. Show that any finite field has prime power order.

Proposition 2.10. *A field of order p^n exists for every prime p and every natural number n, and any two fields with p^n elements are isomorphic.*

3. Roots of Polynomials

As we saw when defining adjoining an element, polynomials, in particular, minimal polynomials, play an important role in the theory.

Proposition 3.1. *Given a polynomial $f \in F[x]$, there exists an algebraic field extension E/F such that f as a root in E*

Proof. Clearly it suffices to show this only for irreducible polynomials. If f is irreducible, $E = F[x]/(f)$, then x is a root of f in E. □

Definition 3.2. A field E is called *algebraically closed* if every polynomial in $E[x]$ has a root in E. If E/F is an algebraic extension, and E is algebraically closed, then E is called an *algebraic closure*. We use $\bar{F}$ to denote an algebraic closure of F.

Theorem 3.3. *Every field has an algebraic closure, and any two algebraic closures of a field are isomorphic.*

Definition 3.4. A polynomial $f \in F[x]$ is called *separable* if it has distinct roots in $\bar{F}$. An extension E/F is called *separable* if, for every $\alpha \in E$, min_α is separable. A field is called *perfect* if every finite extension is seperable.

Proposition 3.5. *Every field of characteristic* 0 *is perfect, as is every finite field.*

So what's an example of a non-separable extension? Take $E = \mathbb{F}_2(\sqrt{t})$ over $F = \mathbb{F}_2(t)$. Then $min_{\sqrt{t}}(x) = x^2 - t = x^2 + t = (x + \sqrt{t})^2$ is not separable. Here's a theorem on finite, separable extensions, called the *Primitive Element Theorem.*

Theorem 3.6. *If E/F is a finite, separable extension, then there is an element $\alpha \in E$, called a* primitive element*, such that $E = F(\alpha)$.*

Definition 3.7. We can an algebraic extension E/F is *normal* if, for every $\alpha \in E$, $min_\alpha(x)$ splits completely into linear factors.

4. Automorphisms and Galois Theory

Definition 4.1. If E and E' are two extensions of F, a *morphism over F* is a F-algebra map $E \to E'$. Note that this is the same as ring map that fixes F pointwise. An *automorphism of E over F* is a isomorphism $E \to E$ that is also a morphism over F. We call the group of automorphisms of E over F the *Galois group of E over F* and denote it by $Gal(E/F)$.

If $\sigma \in Gal(E/F)$ we can extend σ to $E[x] \to E[x]$ by having it act on the coefficients. If $f \in F[x]$ splits into linear factors over $E[x]$, then, since $\sigma(f) = f$, *sigma* must permute the roots of f.

Definition 4.2. An algebraic extension is called *Galois* if it's both normal and separable. If H is a subgroup of $Gal(E/F)$, then the *fixed field of H* is

$$E^H = \{\alpha \in E \mid \sigma(\alpha) = \alpha, \forall \sigma \in H\}$$

Theorem 4.3. (Galois Theory) *Let E/F be a finite Galois extension with Galois group $G = Gal(E/F)$. Let $\mathcal{E}/F = \{\text{Fields } L \mid F \subset L \subset E\}$ and let $\mathcal{O}rb(G) = \{\text{Subgroups of } G\}$. Then the maps*

$$\Phi : \mathcal{E}/F \to \mathcal{O}rb(G)$$
$$K \mapsto Gal(E/L)$$

and

$$\Psi : \mathcal{O}rb(G) \to \mathcal{E}/F$$
$$H \mapsto E^H$$

are inverse maps. Further, a subgroup H is normal in G if and only if E^H is a normal extension of F, and, in that case, $Gal(E^H/F) = G/H$.

A different way to state this is with *category theory.* In this case, the correct definition of $\mathcal{O}rb(G)$ is $\mathcal{O}rb(G) = \{\text{G-sets } G/H \mid H \text{ is a subgroup of } G\}$ with morphisms $\phi : G/H \to G/K$ given by $\phi(gH) = gg'K$, where $g' \in G$ satisfies $g'^{-1}Hg' \subset K$. The statement of Galois theory is as follows.

Theorem 4.4. *The functor*

$$\Psi : \mathcal{O}rb(G)^{op} \to \mathcal{E}/F$$

given by

$$H \mapsto E^H$$

on objects and

$$(gH \mapsto gg'K) \mapsto (\alpha \mapsto g'(\alpha))$$

on morphisms is an isomorphism of categories.