Crash course on fields

Matthew Hase-Liu

Recall that a field K is a commutative ring such that every non-zero element has an inverse. Some examples: $\mathbb{Z}/p\mathbb{Z}$ for p a prime, $\mathbb{R}$, $\mathbb{C}(t)$ (rational functions in one variable—fractions of polynomials in one variable). Note, for instance, that $\mathbb{Z}/10\mathbb{Z}$ is not a field because 2 is a zero-divisor ($2 \cdot 5 = 10 = 0$). Also, $\mathbb{Z}$ is not a field (despite having no zero-divisors) because 123 has no inverse (only 1 and -1 have multiplicative inverses, in fact). Today, we will do a review of algebraic extensions of a field.

1 Characteristic of a field

For any field K (and generally any ring), there is a unique ring homomorphism $\varphi\colon \mathbb{Z} \to K$ given by sending n to $n \cdot 1$. By the first isomorphism theorem for rings, we get $\mathbb{Z}/\ker\varphi \hookrightarrow K$. Since K is a field, $\mathbb{Z}/\ker\varphi$ is an integral domain (has no zero-divisors). Thus $\ker\varphi$ is a prime ideal. It follows that $\ker\varphi$ is of the form $p\mathbb{Z}$, where p is either 0 or a prime number.

Definition 1. For a field K, the number p above is called the **characteristic of** K, and is denoted by $\mathrm{char}(K)$.

Example 2. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ all have characteristic 0 because $\mathbb{Z}$ injects into each of these. $\mathbb{Z}/p\mathbb{Z}$ has characteristic p because the kernel of $\mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ is $p\mathbb{Z}$.

Lemma 3. If K is a field of characteristic p, then K has a subfield isomorphic to $\mathbb{Q}$ if $p = 0$ and $\mathbb{Z}/p\mathbb{Z}$ (and also conversely).

2 Finite and algebraic extensions

Definition 4. Suppose K, L are fields such that $K \subset L$. We say L is a **field extension of** K, and denote this by L/K.

Note that L is a vector space over K, where the scalar action is given by including K into L and then simply multiplying elements in L, i.e. if $a \in K$ and $x \in L$, then ax is defined as multiplying a (viewed in L) with x.

Definition 5. Let L/K be a field extension. Then $[L\colon K] \coloneqq \dim_K L$ is called the **degree of** L **over** K. This is said to be finite/infinite depending on whether the degree is finite/infinite.

Proposition 6. Let $M/L/K$ be a chain of field extensions. Then $[M\colon K] = [M\colon L][L\colon K]$.

Proof. Suppose $[M : L]$ and $[L : K]$ are finite and are equal to m, n. Then, pick a basis $x_1, \ldots, x_m$ of L over K and a basis $y_1, \ldots, y_n$ of M over L. Then, it suffices to show that $\{x_i y_j\}$ (this has mn elements) is a basis of M over K (exercise!). ☺

Definition 7. Let L/K be a field extension. An element $\alpha \in L$ is **algebraic over** K if there is some monic polynomial $p(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0 \in K[x]$ (coefficients are in K) s.t. $p(\alpha) = 0$. Otherwise, α is **transcendental over** K. If every element of L is algebraic over K, we say L/K is an **algebraic extension**.

Example 8. $\sqrt{2} \in \mathbb{R}$ is algebraic over $\mathbb{Q}$ because it satisfies $(\sqrt{2})^2 - 2 = 0$. Of course, it also satisfies $(\sqrt{2})^4 - 4 = 0$, so you might wonder if there is a "minimal" polynomial that works.

Proposition 9. Let L/K be a field extension and $\alpha \in L$ algebraic over K. Then, there is a unique monic polynomial $f \in K[X]$ of smallest degree s.t. $f(\alpha) = 0$. We call f the **minimal polynomial of** α **(over** K**)**.

Proof. Consider the ring homomorphism $\varphi : K[x] \to L$, given by sending a polynomial g to $g(\alpha)$. Since $K[x]$ is a PID (integral domain such that every ideal is generated by a single element), it follows that $\ker \varphi = (f)$ for some unique f (up to a unit). Then, f is precisely the unique monic polynomial of smallest degree s.t. $f(\alpha) = 0$. ☺

Proposition 10. Let $\alpha \in L$ be algebraic over K. Then, write $K[\alpha]$ to denote the subring of L generated by α and K, i.e. the image of $K[x] \to L$ that sends x to α. Then, $K[\alpha]$ is a field and $[K[\alpha] : K] = \deg f$, where f is the minimal polynomial of α.

Proof. We have an isomorphism $K[x]/\ker \varphi \cong \operatorname{im} \varphi = K[\alpha]$. Note that f is irreducible (else $K[x]/(f)$ would have a zero divisor), which implies that (f) is a maximal ideal. Then $K[\alpha] = K[x]/(f)$ is a field. To compute the degree, note that $K[x]/(f)$ has a basis given by $1, x, \ldots, x^{\deg f - 1}$ (if they are not linearly independent, it would contradict the minimality of f). so $[K[\alpha] : K] = \dim_K K[x]/(f) = \deg f$. ☺

Remark 11. In general, we write $K(\alpha)$ to denote the subfield generated by K and α (where $\alpha \in L$ for instance). These extensions are called **simple**. The above proposition says that for α algebraic, we have $K(\alpha) = K[\alpha]$.

Example 12. $\mathbb{Q}[\sqrt[30]{2}]$ has degree 30 over $\mathbb{Q}$. Indeed, $\sqrt[30]{2}$ satisfies $x^{30} - 2 = 0$, which by Eisenstein's criterion is irreducible as a polynomial in $\mathbb{Q}[x]$ (use the prime 2).

Proposition 13. Any finite field extension L/K is algebraic.

Proof. Let $[L : K] = n$ and let $\alpha \in L$. Then, $1, \alpha, \ldots, \alpha^n$ are linearly dependent, so some nontrivial linear combination gives 0, i.e. $c_n\alpha^n + \cdots + c_1\alpha + c_0 = 0$. So α is algebraic. ☺

Corollary 14. *Let L/K be a field extension. Then, TFAE:*

(i) L/K is finite.

(ii) L/K is generated by finitely many elements that are algebraic over K.

(iii) L/K is a finitely generated algebraic field extension.

Remark 15. Not all algebraic extensions are finite. Let $\overline{\mathbb{Q}}$ be the subfield of $\mathbb{C}$ defined as $\{\alpha \in \mathbb{C} : \alpha \text{ is algebraic over } \mathbb{Q}\}$. Then, $\overline{\mathbb{Q}}$ is clearly algebraic over $\mathbb{Q}$. However, $\overline{\mathbb{Q}}$ contains $\mathbb{Q}(\sqrt[n]{2})$ for all n, each of which has degree n over $\mathbb{Q}$. So $\overline{\mathbb{Q}}$ must be infinite.

3 Algebraic closure

For any field K, we want to construct a (minimal) algebraic extension $\overline{K}$ such that any non-constant polynomial in $\overline{K}[x]$ has a root in $\overline{K}$.

Proposition 16. Let K be a field and $f \in K[X]$ a polynomial of degree at least 1. Then, there is a finite algebraic field extension $K \subset L$ such that f admits a zero in L.

Proof. The basic idea is to simply adjoin a root of f to K to get a new field. Suppose f is irreducible. Then, let $L = K[x]/(f)$, which is indeed a field. Then, $K \subset K[x]/(f)$, which is indeed an injection (any ring map between fields is an injection!). Now, $f(x) = 0$ in L by construction, so x is a root of f. ☺

Definition 17. A field K is **algebraically closed** if every non-constant polynomial f of $K[x]$ admits a zero in K, i.e. f splits into linear factors.

Theorem 18. *Every field K admits an extension field L that is algebraically closed and algebraic over K. We say $\overline{K}$ is the **algebraic closure of** K.*

Proof. This isn't quite correct for set-theoretic reasons, but whatever. Let A be the set of all algebraic extensions of K and give it the usual partial order given by inclusion. Zorn's lemma applies, so let $\overline{K}$ be a maximal element. It must be algebraically closed since otherwise we can construct a bigger extension using the Kronecker construction (the proposition) above. ☺

Example 19. We gave an example earlier: $\overline{\mathbb{Q}}$ is an algebraic closure of $\mathbb{Q}$. Last class, we showed that $\mathbb{C}$ is an algebraic closure of $\mathbb{R}$. However, $\mathbb{C}$ is not an algebraic closure of $\mathbb{Q}$, since elements like e and π are not algebraic over $\mathbb{Q}$.

Lemma 20. Let K be a field with α algebraic over K and $f \in K[x]$ the minimal polynomial of α. Let $\sigma\colon K \to L$ be a field homomorphism.

(i) If $\sigma'\colon K(\alpha) \to L$ is a field homomorphism extending σ (i.e. $K \to K(\alpha) \xrightarrow{\sigma'} L$ is the same as σ), then $\sigma'(\alpha)$ is a zero of f^σ (the image of f under the map $K[x] \to L[x]$ induced by σ).

(ii) Conversely, for any root $\beta \in L$ of $f^\sigma \in L[x]$, there is exactly one extension $\sigma'\colon K(\alpha) \to L$ s.t. $\sigma'(\alpha) = \beta$.

In particular, there are at most $\deg f$ different extensions.

Proof. Exercise! Note that $f(\alpha) = 0$ implies $f^\sigma(\sigma'(\alpha)) = \sigma'(f(\alpha)) = 0$ for the first one. For the second one, consider the homomorphisms $K[x] \to K[\alpha]$ and $K[x] \to L$, the former sending g to $g(\alpha)$ and the latter sending g to $g^\sigma(\beta)$, where β is some root in L of f^σ. Then, define σ' as

$K[\alpha] \cong K[x]/(f) \to L$, where the first map is induced by the former and the second is induced by the latter. ☺

Using the above and Zorn's lemma, one can show the following:

Corollary 21. *Let $K \subset K'$ be any algebraic extension and $\sigma\colon K \to L$ be a field homomorphism with image in an algebraically closed field L. Then, σ has an extension $K' \to L$.*

In particular, if K' is algebraically closed and L is algebraic over K, then σ' is an isomorphism.

Corollary 22. *Let L and L' be two algebraic closures of K. Then there is some isomorphism $L \cong L'$ that extends the identity map on K.*

4 Splitting fields

Now, let us begin some preparation for Galois theory. Hopefully the next speaker will say more about this. We care about when polynomials decompose completely into linear factors.

Definition 23. Let f be a non-constant polynomial in $K[x]$. A **splitting field (over K) of f** is a field extension L/K s.t.

(i) f decomposes into a product of linear factors over L.

(ii) L/K is generated by the roots of f.

Remark 24. We can be pretty explicit about this. Let $\overline{K}$ be an algebraic closure of K, and say f has roots $a_1, \dots, a_n$ (say with multiplicity for convenience). Then, $L = K(a_1, \dots, a_n)$ is a splitting field of f over K (since L is generated by the roots and clearly f decomposes as $(x-a_1)\cdots(x-a_n)$).

Proposition 25. Let L_1, L_2 be two splitting fields of a polynomial $f \in K[x]$ of non-constant polynomials, and let $\overline{L_2}$ be an algebraic closure of L_2. Then, any K-homomorphism (i.e. restricts to the identity on K) $\overline{\sigma}\colon L_1 \to \overline{L_2}$ restricts to a K-isomorphism $\sigma\colon L_1 \xrightarrow{\cong} L_2$.

In particular, by the section on algebraic closed fields, we know $K \hookrightarrow \overline{L_2}$ extends to a K-homomorphism $L_1 \to \overline{L_2}$, so any two splitting fields are K-isomorphic.

Proof. Suppose f is monic and f has roots $a_1, \dots, a_n$ in L_1 and $b_1, \dots, b_n$ in L_2. Let $f^{\overline{\sigma}} = \prod(x - \overline{\sigma}(a_i)) = \prod(x - b_i)$, which means $\overline{\sigma}$ maps the set of a_i bijectively onto the set of b_i. Since $L_1 = K(a_1, \dots, a_n)$ and $L_2 = K(b_1, \dots, b_n)$, we get that $L_2 = \overline{\sigma}(L_1)$, i.e. L_1 and L_2 are K-isomorphic. ☺

Everything said above can be extended to f replaced with a (possibly infinite) family of polynomials (f_i).

Theorem 26. *Let L/K be an algebraic extension. Then, TFAE:*

(i) Every K-homomorphism $L \to \overline{L}$ restricts to an automorphism of L.

(ii) L is a splitting field of a family of polynomials (in $K[x]$).

(iii) *Every irreducible polynomial in $K[x]$ that has a root in L decomposes over L into linear factors.*

If these conditions are satisfied, we say L/K is **normal**.

Proof. For (i) implies (iii), let f be an irreducible polynomial with a root $a \in L$. Then, if $b \in \overline{L}$ is any other root, then there is a K-homomorphism $\sigma \colon K(a) \to \overline{L}$ such that $\sigma(a) = b$. Then, we can extend this to $\sigma' \colon L \to \overline{L}$. The assumption of (i) then says that the image of σ' is L, so $b = \sigma'(a) \in L$, so every root of f is in L.

For (iii) implies (ii), let L/K be generated by elements (a_i) and take the family (f_j) of minimal polynomials of the a_i. Then, every root of f_j is in L by the assumption of (iii), so L is the splitting field of (f_j).

For (ii) implies (i), let $\sigma \colon L \to \overline{L}$ be a K-homomorphism. Then, if L is a splitting field, so is $\sigma(L)$, which implies that $\sigma(L) = L$ since they are both subfields of $\overline{L}$. ☺

Remark 27. If $K \subset L \subset M$ is a chain of algebraic extensions, then M/K being normal implies M/L is. Indeed, use the characterization of M as a splitting field.

However, normality is not transitive in a chain: Consider the extensions $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}\left(\sqrt[4]{2}\right)$. We have $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}\left(\sqrt[4]{2}\right)$ are both normal (use the polynomials $x^2 - 2$ and $x^2 - \sqrt{2}$), but $\mathbb{Q} \subset \mathbb{Q}\left(\sqrt[4]{2}\right)$ is not! Indeed, $x^4 - 2$ is the minimal polynomial of $\sqrt[4]{2}$, but it has complex roots (say $i\sqrt[4]{2}$) that are not in $\mathbb{Q}\left(\sqrt[4]{2}\right)$, i.e. $x^4 - 2$ does not split into linear factors.

5 Separable extensions

Hopefully the next speaker will also say something about this! We also care about when roots appear without multiplicity.

Definition 28. Let L/K be a field extension. Then $\alpha \in L$ is called **separable over** K if the minimal polynomial of α, when factored over $\overline{L}$, has no repeated roots. If every $\alpha \in L$ is separable, we say L/K is a **separable extension**.

Moreover, if every algebraic extension of K is separable, we say K is perfect.

There is an easy criterion to check if f has multiple roots:

Lemma 29. The multiple roots of a polynomial $f \in K[x]$ (in some $\overline{K}$) coincide with the common roots of f and f' (the derivative).

In particular, if f is irreducible, it has multiple roots iff f' is identically zero.

Proof. Exercise! ☺

Remark 30. Using the criterion above, every algebraic field extension in characteristic 0 is separable. In particular, all fields of characteristic 0 are perfect! This means the only examples we'll find are over characteristic p.

Example 31. Let p be prime. Then, $x^p - t \in \mathbb{F}_p(t)[x]$ is irreducible but not separable (i.e. a polynomial with only simple roots). Indeed, the derivative is $px^{p-1} = 0$, which is identically zero. In other words, the extension $\mathbb{F}_p(t)[x]/(x^p - t)$ is not separable over $\mathbb{F}_p(t)$.

Let us now give a characterization of separable extensions.

Definition 32. For an algebraic field extension L/K, denote by $\operatorname{Hom}_K(L, \overline{K})$ the set of K-homomorphisms from L into an algebraic closure $\overline{K}$. Then, define

$$[L : K]_s := \# \operatorname{Hom}_K(L, \overline{K}).$$

As usual, this is easy to understand in the case of a simple extension:

Lemma 33. Let $K \subset K(\alpha) = L$ with f the minimal polynomial of α.

(i) $[L : K]_s$ is the number of distinct roots of f (in $\overline{K}$).

(ii) α is separable over K iff $[L : K] = [L : K]_s$.

Proof. This is clear from what we've done earlier. Indeed, note that $[L : K] = \deg f$, which is the number of roots (with multiplicity). ☺

Lemma 34. Let $K \subset L \subset M$. Then, $[M : K]_s = [M : L]_s[L : K]_s$.

Proof. Exercise! ☺

Theorem 35. *For a finite field extension $K \subset L$, TFAE:*

(i) L/K is separable.

(ii) There elements $a_1, \ldots, a_n \in L$ separable over K and $L = K(a_1, \ldots, a_n)$.

(iii) $[L : K]_s = [L : K]$.

Proof. (i) implies (ii) is by definition, (ii) implies (iii) follows from the previous two lemmas iteratively. For (iii) implies (i), take $a \in L$ and one can show that $[K(a) : K] = p^r[K(a) : K]_s$ for some r (you can assume K has characteristic p, otherwise there's nothing to show). Then, there is an estimate

$$[L : K] = [L : K(a)][K(a) : K] \geq [L : K(a)]_s p^r [K(a) : K]_s = p^r [L : K]_s,$$

which forces $r = 0$. ☺

Remark 36. This can be extended to all algebraic extensions easily.

One of the most useful properties of separable extensions is the following. We won't prove it, but it is a clever application of pigeonhole:

Theorem 37. *Every finite separable field extension L/K admits a primitive element, i.e. an element $a \in L$ s.t. $L = K(a)$.*

Remark 38. There is also a notion of purely inseparable extensions, but we'll talk about that another time. Instead of $[L : K]_s$ being maximal, we want it to be minimal, i.e. equal to 1, for these extensions. In general, one can factor any extension L/K as $L/K_s/K$, where K_s/K is separable and L/K_s is purely inseparable.

Remark 39. A finite separable extension will eventually be the right notion of an "algebraic" covering space over a point. More precisely, if L/K is such an extension, $\operatorname{Spec} L \to \operatorname{Spec} K$ is a map of "schemes" that is "finite etale" (i.e. an algebraic covering space).

The reason for this is that L/K being finite separable is equivalent to the "cotangent bundle" of $\operatorname{Spec} L \to \operatorname{Spec} K$ being trivial, i.e. $\Omega_{L/K} = 0$. But geometrically this is saying that the maps on tangent spaces are isomorphisms, which is what it means to be a local homeomorphism. So it's all very consistent!

6 Finite fields

This final section is mainly an extended example. We already know that $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is a field, but what about larger finite fields (of size a power of a prime)?

Theorem 40. *Let p be a prime. For every integer n, there is an extension $\mathbb{F}_q/\mathbb{F}_p$ consisting of $q = p^n$ elements. Moreover, $\mathbb{F}_q$ is uniquely characterized as the splitting field of $x^q - x$ over $\mathbb{F}_p$, i.e. the elements of $\mathbb{F}_q$ are the q distinct roots of $x^q - x$.*

Every finite field of characteristic p is isomorphic to some $\mathbb{F}_q$.

Proof. Let $f = x^q - x$. Since $f' = -1$, it follows that f is separable, i.e. has exactly q roots in an algebraic closure $\overline{\mathbb{F}_p}$. By using the binomial formula, one can check that $a+b$ satisfies $(a+b)^q = a+b$ and also that $(ab^{-1})^q = ab^{-1}$, which implies that that the q roots form a subfield of q elements.

To get uniqueness, suppose $\mathbb{F}$ contains $\mathbb{F}_p$ and has q elements. We know the multiplicative group $\mathbb{F}^\times$ is of order $q-1$, so by Lagrange's theorem every non-zero element satisfies $x^{q-1} - 1 = 0$. Then, every element satisfies $x^q - x = 0$ (including 0). So we conclude $\mathbb{F}$ is a splitting field of $x^q - x$ over $\mathbb{F}_p$. ☺

Corollary 41. *Finite fields are perfect.*

Proof. Any finite extension of $\mathbb{F}_q$ looks like $\mathbb{F}_{q^n}$ for size reasons. But $\mathbb{F}_{q^n}$ is a splitting field, so it is normal and separable over $\mathbb{F}_q$. For any algebraic extension, we can write it as a union of its finite subextensions. ☺

Proposition 42. $\overline{\mathbb{F}_q}$ looks like $\bigcup_{n \geq 1} \mathbb{F}_{q^n}$. Exercise!