Math 250A Lecture 19 Notes

Daniel Raban

October 31, 2017

1 Field Extensions

1.1 Field extensions and algebraic elements

Definition 1.1. Let K be a field. A *field extension* L of K is a field such that K is a subfield of L. This is written as $K \subseteq L$ or L/K.

Example 1.1. $\mathbb{C}$ is a field extension of $\mathbb{R}$.

Definition 1.2. The *degree* $[L : K]$ of K/L is $\dim L$ as a vector space over K.

Example 1.2.
$$[\mathbb{C} : \mathbb{R}] = 2.$$

Definition 1.3. An element $\alpha \in L$ is called *algebraic* over K if α is a root of some polynomial in $K[x]$.

Example 1.3. The real number $\sqrt[5]{2}$ is algebraic over $\mathbb{Q}$, as a root of $x^5 - 2$.

Example 1.4. Neither π nor e is algebraic over $\mathbb{Q}$. The proof of this is hard.

In general, it is difficult to prove whether something is algebraic or not. The following are still open problems:

1. Is $e + \pi$ algebraic?

2. Is $e\pi$ algebraic?

Example 1.5. Let $L = \mathbb{Q}(x)$ be the rational functions in x. Then $[L : \mathbb{Q}] = \infty$, and x is not algebraic.

Theorem 1.1. *α is algebraic over K iff α is contained in a finite extension K_1 of K ($[K_1 : K] < \infty$).*

Proof. Suppose $\alpha \in K_1$ with $[K_1 : K] = n < \infty$. Look at $1, \alpha, \alpha^2, \ldots, \alpha^n$. This is $n+1$ elements in an n-dimensional vector space over K, so we get

$$a_1 + a_1\alpha + \cdots + a_n\alpha^n = 0,$$

where $a_i \in K$ and the a_i are not all 0. So α is algebraic.

Suppose that α is algebraic. Then $p(\alpha) = 0$ for some $p \in K[x]$. We can assume p is irreducible. So $K[x]/(p)$ is a field, K_1. So $[K_1 : K] = \deg(p)$, with basis $1, x, x^2, \ldots, x^{\deg(p)-1}$. So we get a map $K[x]/(p) \to L$.

$$\begin{tikzcd}
K[x]/(p) \arrow[r, "x \mapsto \alpha"] & L \\
K \arrow[u] \arrow[ur] &
\end{tikzcd}$$

This map is injective since $K[x]$ is a field, so the image of the map is a field of degree $< \infty$ containing α. $\square$

Lemma 1.1. *Let $K \subseteq K_1 \subseteq K_2$. Then*

$$[K_2 : K] = [K_2 : K_1][K_1 : K].$$

Proof. Let $x_1, \ldots, x_m$ be a basis of K_1 over K, and let $y_1, \ldots, y_n$ be a basis of K_2 over K_1. Then $x_i y_j$ form a basis of K_2 over K (exercise). So $[K_2 : K] = mn$. $\square$

Proposition 1.1. *Suppose $\alpha, \beta \in L$ are algebraic over K. Then so are $\alpha + \beta$ and $\alpha\beta$.*

Proof. Say $\alpha \in K_1$ with $[K_1 : K]$ is finite. β satisfies an irreducible polynomial of degree $n < \infty$ over K, so β satisfies an irreducible polynomial of degree $\leq n$ over K_1. Then β is algebraic over K, say $\beta \in K_2$ with $[K_2 : K_1] < \infty$. Then

$$[K_2 : K] = [K_2 : K_1][K_1 : K],$$

so $[K_2 : K] = [K_2 : K_1][K_1 : K] < \infty$. $\alpha + \beta \in K_2$ and $\alpha\beta \in K_2$, so they are algebraic. $\square$

Example 1.6. $\alpha = \sqrt{2} + \sqrt[3]{2} + \sqrt[5]{2}$ is algebraic. The smallest degree polynomial $p(x)$ with $p(\alpha) = 0$ has degree 30.

Example 1.7. All algebraic elements of $\mathbb{C}$ over $\mathbb{Q}$ form a field.[1]

In general, we have the following fact.

Proposition 1.2. *$K[x]/p(x)$ is a field if p is irreducible.*

[1] This is called the field of algebraic numbers and is studied in algebraic number theory.

Proof. This is a quick consequence of a homework problem we have done, and should be done as an exercise. Use the fact that $K[x]$ is a PID. $\square$

Suppose that p is not irreducible. Then for $p = fg$ for some coprime f, g. Then $K[x]/(p) \cong K[x]/(f) \times K[x]/(g)$ by the Chinese remainder theorem. So if p does not have multiple copies of the same factor, $K[x]/(p)$ is a product of fields. If p has multiple copies of a factor, $K[x]/(p)$ can be strange.

Example 1.8. Let $p = x^n$. Then $K[x]/(x^n)$ is the ring of truncated polynomials of the form $a_0 + a_1 x + \cdots + a_{n-1}x^{n-1}$ with $x^n = 0$ and $a_i \in K$. This has nilpotent elements, so it is not a product of fields.

Suppose that p is an irreducible polynomial in $K[x]$. We can find an extension field L so that p has a root in L, $L = K[x]/(p)$. Does P factorize into linear factors in L? Sometimes.

Example 1.9. Let $p(x) = x^3 - 2$ in $\mathbb{Q}[x]$. This is irreducible by Eisenstein's criterion. Let $L = \mathbb{Q}[x]/(x^3 - 3) = \mathbb{Q}[\sqrt[3]{2}] = \left\{a_0 + a_1\sqrt[3]{2} + a_2(\sqrt[3]{2})^2 : a_i \in \mathbb{Q}\right\}$. Does $x^3 - 2$ factor in linear factors in L? It does not. $L \subseteq \mathbb{R}$, and $x^3 - 2$ only has 1 real root. The others are $\sqrt[3]{2}e^{2\pi i/3}$ and $\sqrt[3]{2}e^{4\pi i/3}$.

Example 1.10. Let $p(x) = x^4 + 1$. This is irreducible; check by sending $x \mapsto x + 1$. We get $x^4 + 4x^3 + 6x^2 + 4x + 2$, which is irreducible by Eisenstein. Look at the complex roots: $e^{\pi i/4}, e^{3\pi i/4}, e^{5\pi i/4}, e^{7\pi i/4}$. So

$$L = \mathbb{Q}[x]/(x^4 + 1) \cong \mathbb{Q}[\zeta] = \left\{a_0\zeta + z_1\zeta + a_2\zeta^2 + z_3\zeta^3 : a_i \in \mathbb{Q}\right\}.$$

In this case, p factors as

$$p(x) = (x - \zeta)(x - \zeta^3)(x - \zeta^5)(x - \zeta^7).$$

1.2 Splitting fields

Definition 1.4. Suppose $p \in K[x]$ with $K \subseteq L$. L is a *splitting field* of p if

1. The polynomial p factors into linear factors in L.
2. L is generated by roots of p.

Example 1.11. $\mathbb{Q}[\zeta]$ is a splitting field of $x^4 + 1$.

Example 1.12. $\mathbb{Q}[\sqrt[3]{2}]$ is not a splitting field of $x^3 - 2$.

How do we find a splitting field? Let's find the splitting field of x^3-2. Form $\mathbb{Q}[\sqrt[3]{2}] = \mathbb{Q}[x]/(x^3-2) = K_1$. In K_1, $x^3-2 = (x-\sqrt[3]{2})(x^2+\sqrt[3]{2}x+(\sqrt[3]{2})^2)$, where the latter factor is in $K_1[x]$. Add the roots of this to K_1, forming $K_1[x]/(x^2+\sqrt[3]{2}x+(\sqrt[3]{2})^2)$.

Here is the general construction of the splitting field of $p \in K[x]$: Factor p. If there are no factors of degree > 1, we are done. Otherwise, pick a factor q, where q is irreducible and of degree > 1. Form a new field $K[x]/(q)$. Over this field, p has one extra linear factor. Repeat this with p/q. We get

$$K \subseteq K_1 \subseteq K_2 \subseteq K_3 \subseteq \cdots \subseteq K_n,$$

where at degree k, we add the root α_k of $p/((x-\alpha_1)\cdots(x-\alpha_{k-1}))$. So

$$[K_n : K] \leq n!$$

using our lemma about degrees. So the splitting field has degree $\leq \deg(p)!$.

The splitting field is essentially unique.

Proposition 1.3. *If L_1, L_2 are 2 splitting fields of K, $L_1 \to L_2$, we can find an isomorphism from $L_1 \to L_2$, fixing all elements of K.*

$$\begin{tikzcd} L_1 \arrow[r] & L_2 \\ K \arrow[u] \arrow[ur] & \end{tikzcd}$$

Proof. As before, construct the sequence of field extensions

$$K \subseteq K_1 \subseteq K_2 \subseteq K_3 \subseteq \cdots \subseteq K_n.$$

Suppose L is a splitting field of K. Then $K_1 \to L$ because $K_1 = K[x]/q_1(x)$, and L is a splitting field of P. We can form maps $K_i \to L$ for each i in this way.

$$\begin{tikzcd} K \arrow[d] & K_1 \arrow[dl] & K_2 \arrow[dll] & \cdots & K_n \arrow[dllll] \\ L & & & & \end{tikzcd}$$

Then the image of K_n is all of L since L is generated by the roots of p. So $K_n \cong L$. $\square$

This isomorphism is not necessarily unique.

Example 1.13. $\mathbb{C}$ is the splitting field of x^2+1 over $\mathbb{R}$. What is $\sqrt{-1}$? It can be i or $-i$, depending on which isomorphism you use.

1.3 Application to finite fields

Proposition 1.4. *For each prime power p^n, there is a unique finite field F_{p^n} with p^n elements.*

Proof. The main idea of the proof is that F_{p^n} is the splitting field of $x^{p^n} - x$.

We first show that the splitting field of $x^{p^n} - x$ has p^n elements. This has p^n roots because the derivative is $p^n x^{p^n-1} - 1$, which is coprime to $x^{p^n} - x$. The key point is is that the roots form a field (closed under addition and multiplication) because $(a+b)^p = a^p + b^p$ in characteristic p, and because the roots are 0 or roots to $x^{p^n-1} = 1$. So the roots form a field of order p^n.

For uniqueness, we want to check that any field of order p^n is a splitting field of $x^{p^n} - x$. The key point here is that all elements are roots of $x^{p^n} - x$. If $x = 0$, it is a root. If $x \neq 0$, then $x \in L^*$ (order $p^n - 1$ and is a group), so $x^{p^n-1} = 1$ by Lagrange's theorem. $\square$

Example 1.14. Let's construct the field of order $2^4 = 16$. We have proved that it exists, but the abstract proof is useless for construction. Find the irreducible factor p of $x^{16} - x$ of degree 4. Form $F_2[x]/p$. Any field of order 16 is a splitting field; for example $F_2[x]/p$ for any irreducible p of degree 4. Any irreducible polynomial in $F[x]$ of degree 4 divides $x^{16} - x$. So

$$x^{16} - x = (x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1)(x^2 + x + 1)(x + 1)x.$$

Note that 1,2, and 4 are the factors of 4.[2] This is divisible by $x^{2^2} - x$ and $x^{2^1} - 1$. To get an explicit construction of the field of order 2^4, use $F_2/(x^4 + x + 1)$, or quotient out by your favorite irreducible polynomial of degree 4 over F_2.[3]

Example 1.15. How many irreducible polynomials are there of degree 6 in $F_2[x]$? We have that

$$x^{2^6} - x = (\text{irred. polys of deg } 6)(\text{irred. polys of deg } 3)(\text{irred. polys of deg } 2)(x + 1)x.$$

Using a kind of inclusion-exclusion argument, we get that the degree of the product of polynomials of degree 6 is $2^6 - 2^3 - 2^2 + 2^1$. Each polynomial has degree 6, so the number of polynomials is $(2^6 - 2^3 - 2^2 + 2^1)/6 = 9$.

1.4 Algebraic closure

Definition 1.5. L is called the *algebraic closure* of K if the following conditions hold:

1. Any element of L is algebraic over K.

[2] You may recall that these are the irreducible polynomials we computed in a previous lecture.

[3] In general, there is no preferred element to quotient out by. This is troublesome, because the fields you obtain are technically different, even though they are isomorphic.

2. Any polynomial in $L[x]$ has a root.

Example 1.16. $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$.

Proposition 1.5. *Any field has an algebraic closure, unique up to isomorphism. More generally, given any set of polynomials in $K[x]$, we can find a splitting field such that:*

1. *All polynomials in the set factorize into linear factors.*

2. *L is generated by the roots of the polynomials.*

Proof. Suppose there are a countable number of polynomials $p_1, p_2, p_3, \ldots$. Form

$$K \subseteq K_1 \subseteq K_2 \subseteq \cdots,$$

where K_n is a splitting field for p_n over K_{n-1}. The union is a splitting field. If we have an uncountable number of polynomials, use the magic words: Zorn's lemma. So we have found $L \supseteq K$ such that all polynomials in $K[x]$ have a root in L; we want that all polynomials in $L[x]$ have a root in L.

Suppose that p is irreducible in $L[x]$, and form $M = L[x]/p(x)$. Then the coefficients of p are all in K, so they all lie in some finite extension of K. So α is contained in a finite extension of K, so α is algebraic over K. This makes $\alpha \in L$ since any polynomial in $K[x]$ splits into linear factors in L.

Uniqueness of the algebraic closure is much like the uniqueness of splitting fields. $\square$

It's difficult to find easy to explain examples of algebraic closures.

Example 1.17. Let K be the field of formal Laurent series over $\mathbb{C}$. This has elements $\cdots + a_{-n}z^{-n} + \cdots + a_0 + a_1 z + \cdots$ with $a_i \in \mathbb{C}$. The algebraic closure is

$$\bigcup_{k \geq 1} \text{formal Laurent series in } z^{1/k}.$$

These are called Puiseux series.[4]

[4] These date back to Newton, but they are not named after him because no one knew what algebraic closures were back then.