Abstract Algebra – III Field extensions (域扩张) and Galois theory (伽罗瓦理论)

3.1 Algebraic and Transcendental Extensions, 3.2 Algebraic closure

December 17, 2012

Outline

Algebraic and transcendental extensions (代数与超越扩张)

Remark

Note that a field F has only two ideals, (0) and F. Therefore every ring-homomorphism from a field is an embedding. So the main part in the study of fields is the study of field extensions.

Definition

Let $F \subset E$ be a field extension. An element $\alpha \in E$ is called algebraic over F (代数的) *if there is a nontrivial polynomial $p \in F[x]$ such that $p(\alpha) = 0$.*
An element that is not algebraic is called transcendental (超越).
A field extension $F \subset E$ is called algebraic if every element in E is algebraic over F.
A field extension that is not algebraic is called transcendental.

Example

1. Consider the number $\sqrt{2} \in \mathbb{R}$. It is algebraic over $\mathbb{Q}$, because it is a root of $x^2 - 2 \in \mathbb{Q}[x]$. We can form the field extension $\mathbb{Q}(\sqrt{2})$ as the subalgebra in $\mathbb{R}$ generated by $\mathbb{Q}$ and $\sqrt{2}$. Since $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{2}) = \deg(x^2 - 2) = 2$ we know that the increasing powers of any element $\alpha \in \mathbb{Q}(\sqrt{2})$ are linear dependent over $\mathbb{Q}$. Therefore $\mathbb{Q}(\sqrt{2})$ is an algebraic extension.
2. Consider $\mathbb{Q}(x)$ the field of rational functions over $\mathbb{Q}$ in one variable. Since x is a free variable, there is no nontrivial polynomial $p \in \mathbb{Q}[x]$ such that $p(x) \equiv 0$. Therefore $\mathbb{Q}(x)$ is a transcendental extension of $\mathbb{Q}$ and x a transcendental element. The same is true for $\mathbb{Q}(\mathrm{e})$ once you have proven that the Euler number e is transcendental.

3. Characteristic of a field $\phi_0 : \mathbb{Z} \to F : n \mapsto n \cdot 1$. We already know $\ker \phi_0 = (n) \lhd \mathbb{Z}$. But moreover $\mathbb{Z}/(n) \cong \operatorname{im} \phi_0 \subset F$ is a subring thus a domain. Therefore (n) a prime ideal, i.e. $\operatorname{char}(F)$ either a prime number or 0. If $Z/(p) \subset F$, then this is the prime field (基本域) of F. If $\operatorname{char}(F) = 0$, then also $\mathbb{Q} = K[\mathbb{Z}] \subset F$. Thus $\mathbb{F}_0 := \mathbb{Q}$.
   In what follows when E is fixed, you can always choose the prime field as F, because it is automatically contained in every subfield $K \subset E$.
4. Note that in any field extension $F \subset E$, E is a vector space over F. If it is a finite dimensional vector space, we denote $[E : F] := \dim_F E$ the algebraic degree (代数度数) of E over F. Analogous to the first example every element in E must be algebraic over F. This justifies the name. Conversely if E/F contains transcendental elements, then its dimension must be infinite.

Proposition (Tower property)

Given algebraic extensions $F \subset K \subset E$, then $[E : F] = [E : K][K : F]$ and in particular $[E : F]$ is infinite iff either $[E : K]$ or $[K : F]$ is infinite.

Proof.

Note that a K-base $\{e_i\}$ of E together with an F-base $\{k_j\}$ of K gives an F-base of E as follows $\{e_i k_j\}$. Thus the dimension fomula follows. □

Definition

Given a field F, then any $f \in F$ for which there is an $n \in \mathbb{N}_+$ with $f^n = 1$ is called a root of unity.

Example

In the complex numbers the n-th roots of unity are $\mathrm{e}^{2\pi \mathrm{i} k/n}$ for $k = 0, \ldots, n-1$. They form a cyclic group with generators any primitive n-th root, e.g. $\omega_n := \mathrm{e}^{2\pi \mathrm{i}/n}$ or more generally any $\mathrm{e}^{2\pi \mathrm{i} k/n}$ as long as k and n are relatively prime.

The latter property is shared among all fields, i.e.

Proposition

Every finite multiplicative subgroup of a field is cyclic and thus consists of roots of unity.

Proof.

Let F be the field in consideration and $G \subset F^*$ be a finite group of order $(G:1) = p_1^{k_1} \cdots p_n^{k_n}$. Since G is abelian, its structure is $G = G_1 \times \cdots \times G_n$ with G_k abelian and of order $p_k^{n_k}$ for distinct primes $p_k \in \mathbb{P}$ and positive integer exponents $n_k \in \mathbb{N}_+$. It remains to show that the G_k are all cyclic. Consider conversely the set of all $\{r \in G : r^{p^j} = 1 \exists j \in \mathbb{N}_+\}$. It consists exactly of G_k iff $p = p_k$. Since G and thus G_k is finite, there is an element $r \in G_k$ of maximum p-power say $K \in \mathbb{N}$. Clearly $\langle r \rangle \subset G_k$ is a cyclic subgroup with $p^K = \operatorname{ord} r \leq (G_k : 1)$. On the other hand the polynomial $x^{p^K} - 1 \in F[x]$ has at most p^K roots in F. But all the elements in G_k are roots of this polynomial and thus roots of unity. Therefore $(G_k : 1) \leq p^K$ and thus $\langle r \rangle = G_k$ and in particular cyclic. □

Subfields

Corresponding to rings we have the following construction:

Lemma

Given a family of subfields $\{F_\alpha : \alpha \in A\}$ *of a field* F*, then their intersection* $\bigcap_{\alpha\in A} F_\alpha \subset F$ *is a sub-field of* F*.*
The union of a non-empty chain of sub-fields
$F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset E$ *is a sub-field of* E*.*

The proof is left as an exercise.

Definition

Given a field extension $F \subset E$*. The* sub-field generated by a subset $S \subset E$ *over* F *is the smallest field* $\bigcap_{S,F\subset K\subset F} K \subset E$ *that contains* F *and all elements of* S*. It is denoted as* $F(S)$*.*

Subfields II

Proposition

Given a field extension $F \subset E$ and a subset $S \subset E$, then the ring $F[S]$ is the set of all finite F-linear combinations of products of elements in S.
The sub-field $F(S)$ generated by F and S is the field of fractions of the domain $F[S]$, i.e. it consists of all the elements $a/b \in E$ with $a, b \in F[S]$ and $b \neq 0$.

Also this proof is left as an exercise.

Subfields III

The last proposition has some immediate consequences:

Corollary

Given a field extension $F \subset E$, a subset $S \subset E$, and some elements $r, \alpha_1, \ldots, \alpha_n \in E$, then

1. *$r \in F[\alpha_1, \ldots, \alpha_n]$ iff there is some polynomial in n indeterminates $p \in F[x_1, \ldots, x_n]$ such that $r = p(\alpha_1, \ldots, \alpha_n)$;*
2. *$r \in F(\alpha_1, \ldots, \alpha_n)$ iff there is some rational function in n indeterminates $f \in F(x_1, \ldots, x_n)$ such that $r = f(\alpha_1, \ldots, \alpha_n)$;*
3. *$r \in F[S]$ iff there are some $\alpha_1, \ldots, \alpha_n \in S$ such that $r \in F[\alpha_1, \ldots, \alpha_n]$;*
4. *$r \in F(S)$ iff there are some $\alpha_1, \ldots, \alpha_n \in S$ such that $r \in F(\alpha_1, \ldots, \alpha_n)$.*

Also the proof of this corollary is left as an exercise.

Subfields IV

Remark

Given a transcendental field extension E/F, then we can analogous to vector spaces introduce a transcendence degree (超越次数) by counting the minimal number of (transcendental) elements required to generate E over F. Analogously to vector spaces this number is independent of the particular transcendence base.

Finally the products of subfields are the following:

Definition

Given a family of sub-fields $F \subset K_\alpha \subset E$, then their composite $\prod_{\alpha\in A} K_\alpha$ *is the subfield of E generated over F by $\bigcup_{\alpha\in A} K_\alpha$.*

Note that this notion is symmetric in the fields K_α. In particular if $F \subset K_{1/2} \subset E$ are two intermediate fields, then $K_1(K_2) = F(K_1, K_2) = K_2(K_1) \subset E$ and correspondingly for more factors.

Exercises I

Exercise

a. Give a short proof to show that there is no field of order 6.
b. What can you say about fields of order 10, 12, 14?
c. Given the example $\mathbb{Q}(\sqrt{2}) \cong \mathbb{Q}(x)/(x^2-2)$ of degree 2 over $\mathbb{Q}$, what would you need to construct a field with 4, 8, 9, 16 elements?

Exercise

Show Lemma 3.1.8, i.e. given a field extension $F \subset E$ and

a. a family of sub-fields $F_\alpha \subset E$, then their intersection $\bigcap_{\alpha \in A} F_\alpha \subset E$ is a sub-field;
b. a directed chain of sub-fields $F = F_0 \subset F_1 \subset F_2 \subset \cdots \subset E$, then their union $\bigcup_{i=0}^{\infty} F_i \subset E$ is a sub-field.

Exercises II

Exercise

Show Proposition 3.1.10, i.e. given a field extension $F \subset E$ together with a subset $S \subset E$, then

a. the ring $F[S]$ consists of all finite F-linear combinations of products of elements of S;
b. the field $F(S)$ is the field of fractions of the domain $F[S] \subset E$.

Exercise

Assuming the result of the previous exercise, show Corollary 3.1.11.

The algebraic closure (代数闭包)

Definition

Given an algebraic element $\alpha \in E \supset F$ of a field extension $F \subset E$. A minimal polynomial for α is a non-constant polynomial $p \in F[x]$ such that $p(\alpha) = 0$ and $\deg p$ *is minimal.*

Example

Consider $\sqrt{2} \in \mathbb{C} \supset \mathbb{Q}$. It is algebraic, because it is a root of $p = x^2 - 2 \in \mathbb{Q}[x]$. Since $\sqrt{2} \notin \mathbb{Q}$, 2 is the smallest degree of a non-trivial polynomial with root $\sqrt{2}$.

Proposition

Given an algebraic element $\alpha \in E \supset F$ in a field extension $F \subset E$. Then the minimal polynomial $p \in F[x]$ of α is irreducible over F and every polynomial $g \in F[x]$ with $g(\alpha) = 0$ is divisible by p.

Minimal polynomial

Proof.

The first part follows, because $ev\colon F[x] \times E \to E$ is a ring homomorphism in the polynomial thus $p = q_1 q_2$ implies $0 = p(\alpha) = q_1(\alpha)q_2(\alpha)$ and since E is a field, $q_1(\alpha) = 0$ or $q_2(\alpha) = 0$. W.l.o.g. the former equality. But then $\deg q_1 = \deg p$ and so $q_2 \in F^*$ a unit and thus p irreducible.
For the second statement note that $F[x]$ is a Euclidean domain Definition 2.4.4 and thus $d := \gcd(p, g)$ has root α. If $\deg d < \deg p$, then p is not minimal, a contradiction. Otherwise $p = ud$ for some unit $u \in F[x]^* = F^*$ and therefore $p|g$. □

Lemma

Given algebraic field extensions $F \subset K \subset E$ together with an F-homomorphism $\phi\colon K \to E$, then there exists an F-automorphism σ of E such that $\phi = \sigma \circ k$, where $k\colon K \hookrightarrow E$ is the embedding of K into E.

Extending field homomorphisms

Proof for finite extensions.

If $[E : K]$ is finitely generated, e.g. $E = K(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_k \in E \setminus K$, then all we have to do is extend the embedding ϕ consistently to $\alpha_1, \ldots, \alpha_n$. Consider thus a minimal polynomial $p \in F[x]$ for α_1. Obviously $p_\phi = p$, because ϕ is the identity on F. On the other hand p may break over K into smaller irreducible factors $p = p_1^{n_1} \cdots p_k^{n_k}$ one of which has root α_1, w.l.o.g. p_1. Then ϕ has to map α_1 to a root of $(p_1)_\phi$ which has the same degree as p_1 and therefore at least one zero. This extends ϕ to an embedding $\tilde{\phi}\colon K(\alpha_1) \to E$. In order to further extend it to E we go inductively over the remaining elements $\alpha_2, \ldots, \alpha_n$. In the last step we obtain an embedding of E into itself which therefore must be an isomorphism. □

For extensions of infinite degree you need something like Zorn's lemma that says that there is a limiting construction $\tilde{\phi}$ that extends to all of E. Details can be found in Appendix B.

The Algebraic closure I

Definition

A field F is called algebraically closed (代数闭包的) *if every polynomial over F of degree at least 1 has a root in F.*

Example (Fundamental theorem of algebra)

Remember from complex analysis that every complex polynomial of degree at least 1 has a complex root. Therefore $\mathbb{C}$ is an algebraically closed field. It means in particular that every polynomial factors uniquely into a product of linear terms where the uniqueness is up to rearrangement and a factor $u \in \mathbb{C}^*$ which can be made unique by requiring $p = p_n(x - x_1) \cdots (x - x_n)$ with p_n the leading coefficient of p and $x_1, \ldots, x_n \in \mathbb{C}$ the roots of p.

The rational numbers $\mathbb{Q}$ on the other hand, have plenty of non-trivial irreducible polynomials, e.g. $x^2 - 2$, because its roots are $\pm\sqrt{2} \notin \mathbb{Q}$. The question is now whether we can make every

The Algebraic closure II

field algebraically closed by adding some numbers. The general idea is the following.

Lemma

Given an irreducible polynomial $p \in F[x]$, then the extension field $E := F[\xi]/(p)$ has a root of p.

Proof.

The obvious root would be ξ, but we first need to make sure, that E is a field. Certainly $F[\xi] \cong F[x]$ is a (the polynomial) ring over F and in particular a principal ideal domain. Moreover $(p) \lhd F[\xi]$ is a principal ideal. Since p is irreducible, (p) is a prime ideal (Proposition 2.3.6-4. But then $(p) \lhd F[x]$ is also a maximal ideal (Proposition 2.4.7) and thus $F[\xi]/(p)$ a field that contains F as a subfield.

The Algebraic closure III

In this sense we can try to construct the algebraic closure of F by adding more and more roots of (irreducible) polynomials over F, but the full proof requires Zorn's lemma.

Theorem

Let F be a field. It has an algebraic closure, *i.e. an algebraic field extension $F \subset \bar{F}$ where $\bar{F}$ is algebraically closed. $\bar{F}$ is unique up to isomorphism of extensions.*

Easier part of the proof I

We assume that there is an extension $F \subset E$ that contains all algebraic elements over F, i.e. for every non-constant polynomial $p \in F[x]$ there is at least one (and thus $\deg p$) element(s) $\alpha \in E$ such that $p(\alpha) = 0$. The difficulty is that E may be too big, i.e. also contain transcendental elements over F. We thus take the set $\mathrm{Alg}(E/F) := \{\alpha \in E : \alpha \text{ is algebraic over } F\} \subset E$ and define $\bar{F} := F(\mathrm{Alg})$. Clearly $\bar{F}$ is algebraic over F. Let $p \in \bar{F}[x]$ be any non-constant polynomial over $\bar{F}$. Since it has only finitely many coefficients, all these coefficients are contained in a finite (algebraic) extension $F \subset F_p \subset \bar{F}$. Now there is a field $E_p \supset F_p$ of finite degree that contains a root of $p \in F_p[x]$. But since $[F_p : F]$ as well as $[E_p : F_p]$ are finite, so is $[E_p : F] = [E_p : F_p][F_p : F]$ and therefore every element in E_p including any root of p is algebraic over F. Thus there is a root of p in $\bar{F}$.

Easier part of the proof II

In this way there is an embedding of every algebraic element α over F in any algebraic closure of F. But this embedding can be made into a ring-homomorphism that extends the isomorphism of the base field F and thus it is an embedding homomorphism with an inverse and therefore an isomorphism of any two algebraic closures of F. □

The part about the existence of any such E is postponed to Appendix B as it needs a better understanding of Zorn's lemma (which is not in the focus of this course).

Example

1. The algebraic numbers $\bar{\mathbb{Q}}$ are all complex numbers that are algebraic over $\mathbb{Q}$. It is an algebraically closed field, the algebraic closure of $\mathbb{Q}$. Note that this is strictly smaller than $\mathbb{C}$, because of transcendental numbers such as e and π.
2. Consider the real numbers $\mathbb{R}$. We know that the only irreducible polynomials over $\mathbb{R}$ are quadratic polynomials $x^2 + px + q$ with negative discriminant $D := p^2 - 4q < 0$. But these all have complex roots. Therefore $\mathbb{C}$ is the algebraic closure of $\mathbb{R}$.

The isomorphism of all algebraic closures of any fixed field F also implies the following:

Corollary

Given any algebraic field extension $f_0 \colon F \hookrightarrow E$ and any F-homomorphism $\phi \colon E \to \bar{F}$, i.e. $\phi \circ f_0 = (\bar{f} \colon F \hookrightarrow \bar{F})$, then there is an F-automorphism $\sigma \in \mathrm{Aut}_F(\bar{F})$ such that $\phi = \sigma \circ e_0$ with $e_0 \colon E \hookrightarrow \bar{E} = \bar{F}$. □

In the following lectures we will thus assume that for every given field F there is always a smallest field $\mathbb{F}_p \subset F$ ($p \in \mathbb{P}$ a prime or $p = 0$ and $\mathbb{F}_0 := \mathbb{Q}$) as well as a fixed field $\bar{F}$ into which all the algebraic elements over F are embedded.
The previous lemma also permits us to construct for every polynomial $p \in F[x]$ over a field F an algebraic extension $F \subset E_p$ in which p factors into linear terms. Given an algebraic closure $\bar{F}$ we just pick all roots $\alpha_1, \ldots, \alpha_n$ of p in $\bar{F}$ and define $E_p := F(\alpha_1, \ldots, \alpha_n)$ which is a finite extension. This is called the splitting field (分裂域) of p.

Exercises

Exercise

Suppose that a, b are algebraic over the field F (with minimal polynomials) of degree m and n, respectively. What can you say about the degree (of the minimal polynomials) of $a \pm b$, ab, a/b (for $b \neq 0$)?

Exercise

Show that every algebraically closed field is infinite.

Hint: You can assume that over every $\mathbb{F}_p$ ($p \in \mathbb{P}$ a prime) and every positive integer $n \in \mathbb{N}_+$ there is (at least one) an irreducible polynomial of degree n.