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

5. Splitting fields and Normal extensions

December 24, 2012

Outline

Afterword: Separable extensions

Proposition (Theorem of a primitive element, 本原元定理, E. Artin[1])

Let $F \subset E$ be a finite separable extension, then there is an algebraic element $\alpha \in E$ such that $E = F(\alpha)$.

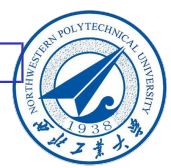
[1] Emil Artin *3/1898, †12/1962

Proof.

If F is finite, then so is E and thus its multiplicative group E^*. But then E^* is cyclic and hence has a generator $\alpha \in E^*$.
If F is infinite, we need to show that every extension $E := F(\alpha, \beta)$ by two algebraic elements is generated by one (algebraic) element. Let $n := [E : F] = [E : F]_s$ and $\phi_1, \ldots, \phi_n$ the F-homomorphisms of E into $\bar{F}$. Let further

$$p := \prod_{i<j} (\phi_i(\alpha) + \phi_i(\beta)x - \phi_j(\alpha) - \phi_j(\beta)x) \in \bar{F}[x].$$

Since F is infinite, we cannot have $p(t) \equiv 0$ for all $t \in F$. Let $t \in F$ be such that $p(t) \neq 0$. But then $\phi_1(\alpha + t\beta), \ldots, \phi_n(\alpha + t\beta)$ must all be distinct. Hence there are at least n F-homomorphisms of $F(\alpha + t\beta) \subset E$ into $\bar{F}$. But then $[F(\alpha + t\beta) : F]_s \geq [E : F]_s$ and so $F(\alpha + t\beta) = E$ as required. □



Afterword: Separable extensions III

Corollary

Let $F \subset E$ be a separable algebraic extension and for every $\alpha \in E$, $\mathrm{Irr}(\alpha/F)$ have degree at most n. Then E/F is finite and $[E:F] \leq n$.

Proof.

Let $\alpha \in E$ be such that $m := \deg \mathrm{Irr}(\alpha/F)$ is maximal. For every $\beta \in E$, we have $F(\alpha,\beta) = F(\gamma)$ for some $\gamma \in E$. But then $\deg \mathrm{Irr}(\gamma/F) \leq m$ and so $[F(\gamma):F] \leq m$. Since $F(\alpha) \subset F(\gamma)$ and $[F(\alpha):F] = m$, we have $F(\gamma) = F(\alpha)$ and so $\beta \in F(\alpha)$, i.e. $F(\alpha) = E$ and in particular $[E:F] = [F(\alpha):F] = m \leq n$. □

Resultants (结式) and discriminants (判别式)
Exercises

Exercise

When do $x^2 + ax + b$ and $x^2 + px + q \in F[x]$ have common roots?

Exercise

Verify the formula for the discriminant of $x^4 + rx^2 + sx + t$.

Exercise

Write the symmetric function
$p_d(x_1, \ldots, x_n) := x_1^d + \cdots + x_n^d \in F[x_1, \ldots, x_n]$ as a polynomial $\bar{f} \in F[s_1, \ldots, s_n]$ in the elementary symmetric functions

a. for $d = 2$,

b. for $d = 3$,

c. for arbitrary $d \in \mathbb{N}$.

Exercise

We know that for quadratic polynomials $x^2 + px + q \in \mathbb{R}[x]$ the polynomial factors over $\mathbb{R}$ iff the discriminant $D := p^2 - 4q$ fulfills $D \geq 0$. What is the corresponding condition for quadratic polynomials over arbitrary fields F not of characterisitc 2?

Splitting fields and Normal extensions (正规扩张)

Remember that the *splitting field (分裂域)* E_p of a polynomial $p \in F[x]$ over a field F is the algebraic extension of F by all roots of p in $\bar{F}$.
These splitting fields have an interesting property:

Proposition

Let $F \subset E$ be the splitting field of a polynomial $p \in F[x]$, then

1. *every F-homomorphism $\phi\colon E \to \bar{F}$ has $\phi(E) = E$,*
2. *every irreducible polynomial over F that has a root in E splits into linear factors over E.*

Splitting fields and Normal extensions (正规扩张) II

Proof.

"1" Note that every F-homomorphism leaves F invariant and thus maps p to itself and therefore also all its roots in E to roots in $\bar{F}$ of the same p. But all these roots are in E. Since E is generated by all these roots, $\phi(E) = E$.

"2" Suppose thus that $q \in F[x]$ is an irreducible polynomial and has a root $\alpha \in E$. But due to Proposition 3.3.4, there are F-automorphisms of $\bar{F}$ that map the root α to every other root of q. Each of those automorphisms restricts to a homomorphism of E into $\bar{F}$ and by the first part map $\phi(E) = E$. But then every other root of q is also in E, i.e. q splits into linear factors over E. □

Splitting fields and Normal extensions (正规扩张) III

Example

Note however, that this is not true for arbitrary field extensions. Let $E := \mathbb{Q}(\sqrt[3]{2})$ and $p = x^3 - 2 \in \mathbb{Q}[x]$ which is an irreducible polynomial over $\mathbb{Q}$. It has a root in E, namely $\sqrt[3]{2}$, but splits here only into $p = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4})$ and the latter is irreducible over E, because its roots $\mathrm{e}^{\pm 2i\pi/3}\sqrt[3]{2}$ are not in E.

We therefore define.

Definition

A field extension $F \subset E$ is called normal (正规的) *if every irreducible polynomial in F that has a root in E splits into linear factors over E.*

Actually the first proposition is an equivalence if we either restrict to extensions of finite degree or consider splitting fields of arbitrary families of polynomials over F.

Splitting fields and Normal extensions (正规扩张) IV

A property we will need for the Galois correspondence principle is the following:

Lemma (Normal tower)

Given a normal field extension $F \subset E$, then for every intermediate field $F \subset K \subset E$ the extension $K \subset E$ is also normal.

Proof.

If E is the splitting field of the (family of) polynomial(s) $p \in F[x]$, then it is also the splitting field of the same polynomials over K. □

Remark

Note however that the other three cases can be wrong, i.e. neither K/F need to be normal nor does K/F and E/K being normal imply that E/F is normal.

Splitting fields and Normal extensions (正规扩张) V

Remark

Analogous to normal subgroups it is also possible to define the normal closure (正规闭包) of an itermediate field $F \subset K \subset \bar{F}$ as the smallest normal extension of F in $\bar{F}$ that contains K, because the intersection of normal extensions is normal again.
Correspondingly this normal closure is generated (as the composite field) by all conjugates of K in $\bar{F}/F$, i.e. the image of K under F-automorphisms of $\bar{F}$.

Exercises

Exercise

Find counter examples for the Remark 3.5.5, i.e.

0. a normal field extension $F \subset E$ together with an intermediate field $F \subset K \subset E$ such that K/F is not normal;
a. two normal field extensions $F \subset K$ and $K \subset E$ such that E/F is not normal.

Exercise (Structure of finite fields)

Show that $\mathbb{F}_{p^m}$ and $\mathbb{F}_{p^n}$ are embedded in $\mathbb{F}_{p^l}$ with $l = \mathrm{lcm}(m, n)$ and their intersection (in the embedding) is $\mathbb{F}_{p^d}$ with $d = \gcd(m, n)$. Conclude that $\bar{\mathbb{F}}_p$ is the inductive limit $\bar{\mathbb{F}}_p = \varinjlim_n \mathbb{F}_{p^n}$, what are the embeddings $\mathbb{F}_{p^m} \hookrightarrow \mathbb{F}_{p^n}$ (i.e. for which m and n do they exist)?

Exercise

Consider a field $F \subset \bar{F}$ together with a family of intermediate fields $F \subset E_\alpha \subset \bar{F}$ and prove the following:

a. if all E_α are normal over F, then so is their intersection;

b. the normal closure of an algebraic extension $F \subset K \subset \bar{F}$ is the composite of all conjugates of K, i.e. the images of K under all F-automorphisms of $\bar{F}$.