Abstract Algebra – III Field extensions (域扩张)

and Galois theory (伽罗瓦理论)

9. Norm and Trace

2013 年 1 月 05 日

3.8 Solvability by radicals (可解用根式)

Open point: If $\mathrm{Gal}(E : F)$ is cyclic of degree n and F contains all n-th roots of unity, then $E = F(\alpha)$ for some $\alpha \in E$ with $\alpha^n \in F$. Requires norms.

Exercises for 3.8 I

Exercise

a. Find $\Phi_n \in \mathbb{Q}[x]$ for all $n \leq 10$,

b. Find Φ_{12} and $\Phi_{18} \in \mathbb{Q}[x]$.

Exercise

a. Show that $\Phi_n(0) = \pm 1$,

b. show that $\Phi_{2k+1}(0) = 1$ if $k \geq 1$.

Remark (Warning)

Not for every Φ_n are all the coefficients $0, \pm 1$. Unfortunately to find a counter example requires to search among the irreducible factors of $x^n - 1 \in \mathbb{Q}[x]$.

Exercise

Exercises for 3.8 II

Let $p^2|n$ for some prime $p \in \mathbb{P}$. Show that the sum of all complex primitive n-th roots of unity is 0.

Exercise

a. Show that $\mathbb{Q}(\omega_m)\mathbb{Q}(\omega_n) = \mathbb{Q}(\omega_l)$ where $l = \text{lcm}(m, n)$ is the least common multiple.

b. Show that $\mathbb{Q}(\omega_m) \cap \mathbb{Q}(\omega_n) = \mathbb{Q}(\omega_d)$ where $d := \gcd(m, n)$ is the greatest common divisor.

Exercise

Find the smallest $n \in \mathbb{N}$ such that $\text{Gal}(\mathbb{Q}(\omega_n) : \mathbb{Q})$ is not cyclic.

Exercise*

Prove that every finitely generated module[1] over any division ring has a finite basis and that all bases have the same cardinality (number of elements).

Exercise

Using the results of the previous Exercise 3.8.6 show that for a tower of division rings $D \subset K \subset E$, $\dim_D E = (\dim_D K)(\dim_K E)$ and in particular the left side is infinite iff at least one of the two factors on the right side is infinite.

[1] the analogue of a vector space

Exercise

Show the tower properties of radical extensions, i.e.

a. Given a tower of finite algebraic extensions $F \subset K \subset E$, then E/F is a radical extension iff K/F and E/K are radical extensions.

b. If $K \subset E$ is a radical extension and $E, F \subset L$, then EF/KF is a radical extension.

Norm (赋范) and trace (迹) I

Definition

Given a ring R. A norm/valuation *is a map $n\colon R \to (-\infty, \infty)$ with the property that $n(\alpha) = 0$ iff $\alpha = 0$, and $n(\alpha\beta) = n(\alpha)n(\beta)$.*
Given an algebra A over a field F. A norm is a map $n\colon A \to F$ with the property $n(\alpha) = 0$ iff $\alpha = 0$, and $n(\alpha\beta) = n(\alpha)n(\beta)$.

Example

Given a finite dimensional field extension $F \subset E$. We consider the F-linear map $M_\alpha\colon E \to E : v \mapsto \alpha v$ of multiplication with $\alpha \in E$.
The determinant $N\colon E \to F : \alpha \mapsto \det M_\alpha$ of M_α is an element in F and moreover N a norm, because
$\det M_{\alpha\beta} = \det(M_\alpha M_\beta) = (\det M_\alpha)(\det M_\beta)$ and $\det M_\alpha = 0$ implies that α is a zero-divisor, hence 0.
The operation $\alpha \mapsto \operatorname{tr} M_\alpha$ is a trace.

Remark

Norm (赋范) and trace (迹) II

Note that the existence of a norm implies that the ring is a domain. The normed algebras are also called division algebras, because every non-zero element has an inverse if there is an identity in the algebra.

Example

The *real division algebras* are $\mathbb{R}$, $\mathbb{C} = \mathbb{R}(\mathrm{i})$, $\mathbb{H} = \mathbb{R}(\mathrm{i}, \mathrm{j})$, and $\mathbb{O} = \mathbb{R}(\mathrm{i}, \mathrm{j}, \mathrm{E})$ (Octonions, discovered by Graves[2] and independently by Cayley[3]). While $\mathbb{R}$ is linear ordered, $\mathbb{C}$ is algebraically closed, $\mathbb{H}$ is associative but not commutative, and $\mathbb{O}$ is not even associative.

The question may occur what is the relation of norm/ trace to the Galois/ automorphism group of the extension. This is answered with the following two statements:

[2] John T. Graves *1806/12 Dublin/Ireland, †1870/3

[3] Arthur Cayley *1821/8 in London/GB, †1895/1

Lemma

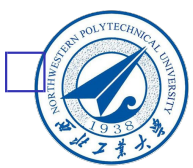
If $F \subset E$ is a finite extension of degree n, $\alpha \in E$ and $q = \mathrm{Irr}_F(\alpha)$ the monic minimal polynomial of α of degree d, then

$$\det(x\mathbb{1} - M_\alpha) = q^{n/d}$$

where in particular d divides n.

Proof.

Remember that for every $a \in F$, $M_{a\alpha} = aM_\alpha$, as well as for $\beta \in E$, $M_{\alpha+\beta} = M_\alpha + M_\beta$. Hence $f(M_\alpha) = M_{f(\alpha)}$ for every $f \in F[x]$. In particular $q(M_\alpha) = M_{q(\alpha)} = 0$, i.e. q is the minimal polynomial of M_α. As opposed to arbitrary minimal polynomials, we know in addition that q is irreducible. In the factorization of ch_A into irreducible polynomials over F, we see that each factor is divisible by the minimal polynomial q of one of its roots and thus $\mathrm{ch}_A = p_A^{n/d}$.



Proposition

Let $F \subset E$ be a finite extension of degree n and $\alpha_1, \ldots, \alpha_s \in \bar{F}$ be the distinct conjugates of $\alpha \in E$. Let further $\phi_1, \ldots, \phi_t$ be the distinct F-homomorphisms of E into $\bar{F}$. Then s and t divide n as well as

$$N(\alpha) = (\alpha_1 \ldots \alpha_s)^{n/s} = (\phi_1(\alpha) \ldots \phi_t(\alpha))^{n/t},$$
$$\mathrm{tr}(\alpha) = \tfrac{n}{s}(\alpha_1 + \cdots + \alpha_s) = \tfrac{n}{t}(\phi_1(\alpha) + \cdots + \phi_t(\alpha)).$$

Some books use these properties as definition of norm and trace. The linearity of the trace as well as the multiplicativity of the norm follow then from the homomorphism properties of the maps ϕ_k.

Proof.

The conjugates α_k of $\alpha \in E$ are the roots of its minimal polynomial $q = \mathrm{Irr}(\alpha/F)$ which all have the same multiplicity m, i.e.

$$q = (x-\alpha_1)^m \cdots (x-\alpha_s)^m = x^{ms} - m(\alpha_1 + \cdots + \alpha_s) + \cdots + (-1)^{ms}(\alpha_1 \ldots \alpha_s)$$

But then $ms = [F(\alpha) : F]$ divides $n = [E : F]$ with $l := [E : F(\alpha)] = \frac{n}{ms}$. So by the previous lemma $\det(x\mathbb{1} - M_A) = q^l$ with the absolute term

$$(-1)^n N(\alpha) = (-1)^{lms}(\alpha_1 \ldots \alpha_s)^{ml}.$$

The linear term is

$$-\operatorname{tr}(\alpha) = -lm(\alpha_1 + \cdots + \alpha_s).$$

Finally let $t := [E : F]_s$ the separability degree of $F \subset E$. We know that $t|n$ as well as $k := [E : F(\alpha)]_s = \frac{t}{s}$. But then

$$\phi_1(\alpha)\dots\phi_t(\alpha) = (\alpha_1\dots\alpha_s)^k$$

as well as

$$\phi_1(\alpha) + \dots + \phi_t(\alpha) = k(\alpha_1 + \dots + \alpha_s).$$

This completes the proof. □

Corollary

Let $F \subset E$ be a finite extension of degree d and $\alpha \in E$. Then N and tr *simplify as follows:*

1. *For $a \in F$, then $N(a) = a^n$, $\mathrm{tr}(a) = na$.*
2. *If $E = F(\alpha)$ is separable, then $N(\alpha) = \alpha_1\dots\alpha_n$ and $\mathrm{tr}(\alpha) = \alpha_1 + \dots + \alpha_n$ where α_k are the conjugates of α.*
3. *If E is not separable, then $\mathrm{tr} \equiv 0$.*
4. *If $F \subset E$ is Galois with Galois group G, then*

$$N(\alpha) = \prod_{\sigma\in G} \sigma(\alpha), \qquad \mathrm{tr}(\alpha) = \sum_{\sigma\in G} \sigma(\alpha).$$

The proof is left as an exercise.

As shown in the last proposition, norm and trace depend on the separability degree of the finite extension $F \subset E$. So it is not surprising that it fulfills similar tower properties as the separability degree:

Proposition (Tower property)

Let $F \subset K \subset E$ be finite extensions. Then

$$N_F^E(\alpha) = N_F^K(N_K^E(\alpha)),$$
$$\mathrm{tr}_F^E(\alpha) = \mathrm{tr}_F^K(\mathrm{tr}_K^E(\alpha))$$

for all $\alpha \in E$.

Also this proof is left as an exercise.

The gap in the proof of radical solutions

Missing property of a cyclic extension: $\mathrm{Gal}(E:F) \cong C_n$ cyclic, then $E = F(\alpha)$ with $\alpha \in E$ and $\alpha^n \in F$ for $\mathrm{char}\, F = 0$.

Lemma

Let $F \subset K \subset E$ be field extensions. The distinct F-homomorphisms of K into E are linearly independent over E.

Proof.

Assume there is an equality $c_1\phi_1 + \cdots + c_n\phi_n = 0$ in which not all the $c_k \in E$ vanish and $\phi_1, \ldots, \phi_n$ are distinct F-homomorphisms of K into E. Among those relations there is one in which n is smallest, i.e. all $c_k \neq 0$ and $n \geq 2$. Then

$$c_1\phi_1(\alpha)\phi_1(\beta) + \cdots + c_n\phi_n(\alpha)\phi_n(\beta) = (c_1\phi_1 + \cdots + c_n\phi_n)(\alpha\beta) = 0,$$
$$c_1\phi_n(\alpha)\phi_1(\beta) + \cdots + c_n\phi_n(\alpha)\phi_n(\beta) = \phi_n(\alpha)(c_1\phi_1 + \cdots + c_n\phi_n)(\beta) = 0$$

for all $\alpha, \beta \in K$. Their difference is

$$c_1(\phi_1 - \phi_n)(\alpha)\phi_1(\beta) + \cdots + c_n(\phi_{n-1} - \phi_n)(\alpha)\phi_{n-1}(\beta) = 0.$$

Since this is a function in $\beta \in K$, we also obtain

$$c_1(\phi_1 - \phi_n)(\alpha)\phi_1 + \cdots + c_n(\phi_{n-1} - \phi_n)(\alpha)\phi_{n-1} = 0.$$

But this means that we have found a (nontrivial) algebraic relation with less homomorphisms, which is a contradiction. □

Lemma (Hilbert's[4] Theorem 90)

Let $F \subset E$ be a cyclic extension and τ a generator of $\mathrm{Gal}(E:F)$, *then for every $\alpha \in E$ we have the following two properties*

1. $N(\alpha) = 1$ *iff* $\alpha = \tau(\gamma)/\gamma$ *for some* $\gamma \in E^*$,
2. $\mathrm{tr}(\alpha) = 0$ *iff* $\alpha = \tau(\gamma) - \gamma$ *for some* $\gamma \in E$.

Proof.

Let G be the Galois group of $E:F$. If $\gamma \in E^*$, then

$$N(\tau\gamma) = \prod_{\sigma \in G} \sigma \circ \tau(\gamma) = \prod_{\sigma \in G} \sigma(\gamma) = N(\gamma).$$

Hence for $\gamma \neq 0$, we have $N(\tau\gamma/\gamma) = 1$.

[4] David Hilbert *1/1862 in Kaliningrad (then Prussia), †2/1943

Conversely assume that $N(\alpha) = 1$. By the previous lemma we know that $\mathrm{Id}, \tau, \tau^2, \ldots, \tau^{n-1}$ are E-linearly independent when $n = [E : F]$. But then

$$\phi := \mathrm{Id} + \alpha\tau + \alpha\tau(\alpha)\tau^2 + \cdots + \alpha\tau(\alpha)\ldots\tau^{n-2}(\alpha)\tau^{n-1} \neq 0$$

as well as

$$\delta := \phi(\beta) \neq 0$$

for some $\beta \in E$. Since

$$N(\alpha) = \alpha\tau(\alpha)\ldots\tau^{n-1}(\alpha),$$
$$\alpha\tau(\delta) = \alpha\tau(\beta) + \alpha\tau(\alpha)\tau^2(\beta) + \cdots + \alpha\tau(\alpha)\ldots\tau^{n-1}(\alpha)\beta = \delta$$

Hence $\alpha = \tau(\gamma)/\gamma$ for $\gamma = \delta^{-1}$.

Similarly for $\gamma \in E$ we obtain

$$\mathrm{tr}(\tau\gamma) = \sum_{\sigma \in G} \sigma \circ \tau(\gamma) = \sum_{\sigma \in G} \sigma(\gamma) = \mathrm{tr}(\gamma)$$

and so $\mathrm{tr}(\tau\gamma - \gamma) = 0$.
Conversely assume that $\mathrm{tr}(\alpha) = 0$. Again $\mathrm{Id}, \tau, \ldots, \tau^{n-1}$ are E-linearly independent and so

$$\mathrm{tr} = \mathrm{Id} + \tau + \cdots + \tau^{n-1} \neq 0$$

as well as

$$\mathrm{tr}(\beta) \neq 0$$

for some $\beta \in E$. Let now

$$\begin{aligned}\delta := \alpha\tau(\beta) + (\alpha + \tau(\alpha))\tau^2(\beta) + \cdots + (\alpha + \tau(\alpha) + \ldots \\ + \tau^{n-2}(\alpha))\tau^{n-1}(\beta)\end{aligned}$$

and observe that

$$\tau(\delta) = \tau(\alpha)\tau^2(\beta) + (\tau(\alpha) + \tau^2(\alpha))\tau^3(\beta) + \cdots - \alpha\beta$$

where in the last term we used $\mathrm{tr}(\alpha) = 0$ as well as $\tau^n = \mathrm{Id}$. Hence

$$\delta - \tau(\delta) = \alpha\tau(\beta) + \alpha\tau^2(\beta) + \cdots + \alpha\tau^{n-1}(\beta) = \alpha\,\mathrm{tr}(\beta)$$

and so $\alpha = \tau(\gamma) - \gamma$ for $\gamma = -\delta/\,\mathrm{tr}(\beta)$. □

Lemma

If $\mathrm{Gal}(E : F)$ *is cyclic of degree* n *and* F *contains all* n*-th roots of unity, then* $E = F(\alpha)$ *for some* $\alpha \in E$ *with* $\alpha^n \in F$.

Remark

If you wish to extend the Galois theorem about solvability of polynomial equations by radical expressions to fields not of characteristic 0, then you need a Property corresponding to the last Lemma. It turns out that the original statement holds as long as the extension degree $n = [E : F]$ is not divisible by the characteristic. If it is, the corresponding property is the Artin–Schreier Theorem and it also replaces the standard polynomial for root extensions by $x^n - x - b \in F[x]$.

Exercises

Exercise

Find N for $E := \mathbb{Q}(\alpha) \subset \mathbb{C}$ with

a. $\alpha = \sqrt{n}$ for some $n \in \mathbb{N}^*$,

b. $\alpha = \mathrm{i}\sqrt{n}$ for some $n \in \mathbb{N}^*$,

c. $\alpha = \sqrt{2} + \sqrt{3}$,

d. $\alpha = \sqrt{2} + \mathrm{i}\sqrt{3}$.

Exercise

Define the unit octonions as
$\mathbb{O}_1 := \langle -1, \mathsf{i}, \mathsf{j}, \mathsf{E} : \mathsf{i}^2 = -1 = \mathsf{j}^2 = \mathsf{E}^2, (-1)^2 = \mathrm{id}, \ldots \rangle_{\mathbb{O}}$ together with the multiplication law

id	i	j	k	E	I	J	K
i	-1	k	$-$j	I	$-$E	$-$K	J
j	$-$k	-1	i	J	K	$-$E	$-$I
k	j	$-$i	-1	K	$-$J	I	$-$E
E	$-$I	$-$J	$-$K	-1	i	j	k
I	E	$-$K	J	$-$i	-1	$-$k	j
J	K	E	$-$I	$-$j	k	-1	$-$i
K	$-$J	I	E	$-$k	$-$j	i	-1

a. Check that $\langle u, v\rangle_{\mathbb{O}}$ for any $u, v \in \mathbb{O}_1$ forms a multiplicative set isomorphic to a subgroup of the unit quaternions and thus is a group (including associativity),
b. Note that $\mathbb{O}_1$ is not associative (thus does not form a group). Check that instead it fulfills the alternative laws

$$(uv)v = u(vv),$$
$$(uu)v = u(uv)$$

for all $u, v \in \mathbb{O}_1$.
c. Define $\mathbb{O} := \mathbb{R}[\mathbb{O}_1]/(-\mathrm{id} = -1)$ where $\mathbb{O}$ is an $\mathbb{R}$-algebra and conclude that it fulfills the same alternative laws. Note that $\langle u, v\rangle_{\mathbb{O}}$ for $u, v \in \mathbb{O}$ generates a subalgebra isomorphic to a subalgebra of the quaternions (thus being associative).
d. Define the norm of an octonion as $|z|^2 := z\bar{z}$ for $z \in \mathbb{O}$ and $\overline{\pm 1} = \pm 1$, $\bar{\imath} = -\mathsf{i}$, $\bar{\jmath} = -\mathsf{j}$, $\bar{\mathsf{E}} = -\mathsf{E}$ and correspondingly for the other units. Verify that $|zw| = |z|\,|w|$ as well as $|z| = 0$ iff $z = 0$.
e. Conclude that $\mathbb{O}$ is a division algebra. (What are the inverse elements?)

Exercise*

Show the simplified formulas for trace and norm in Corollary 3.9.6, i.e. let $F \subset E$ be an extension of finite degree.

a. For $a \in F$, then $N(a) = a^n$, $\mathrm{tr}(a) = na$.

b. If $E = F(\alpha)$ is separable, then $N(\alpha) = \alpha_1 \dots \alpha_n$ and $\mathrm{tr}(\alpha) = \alpha_1 + \cdots + \alpha_n$ where α_k are the conjugates of α.

c. $\mathrm{tr} \equiv 0$ iff E is not separable over F.

d. If $F \subset E$ is Galois with Galois group G, then

$$N(\alpha) = \prod_{\sigma \in G} \sigma(\alpha),$$

$$\mathrm{tr}(\alpha) = \sum_{\sigma \in G} \sigma(\alpha).$$

Exercise

Show the tower properties for norm and trace, i.e. let $F \subset K \subset E$ be finite extensions, then

$$N_F^E(\alpha) = N_F^K(N_K^E(\alpha)),$$
$$\mathrm{tr}_F^E(\alpha) = \mathrm{tr}_F^K(\mathrm{tr}_K^E(\alpha))$$

for every $\alpha \in E$.

Exercises for 3.10

Exercise*

Find the construction of the regular 17-gon with ruler and compass.

Exercise

Given a unit line segment and ruler and compass, show that the following are constructible

. rational numbers,

a. the imaginary unit i,

b. given a line segment of length $a > 0$, then $\sqrt{a}$ is constructible,

c. given a point $z \in \mathbb{C}$, then the point $\sqrt{z} \in \mathbb{C}$, i.e. each of the two square roots are constructible.