Abstract Algebra – III Field extensions (域扩张)

and Galois theory (伽罗瓦理论)

6. Galois extensions and the Correspondence principle

2012 年 12 月 26 日

Galois extensions (伽罗瓦扩张) and the correspondence principle (对应原理)

Lemma

$\mathbb{Q}$ and the prime fields $\mathbb{F}_p$ for $p \in \mathbb{P}$ a prime have no automorphisms.

Proof.

The reason is that $\mathbb{Q}$ and $\mathbb{F}_p$ are the smallest fields generated only by 1. Namely let $\phi\colon \mathbb{Q} \to \mathbb{Q}$ be a ring homomorphism. In particular $\phi(1) = 1$. But then $\phi(n\alpha) = n\phi(\alpha)$ by induction. But this implies that $\phi(p/q) = p/q$ and thus ϕ is the identity on $\mathbb{Q}$.
The arguments for the other fields are analogous. □

Galois extensions (伽罗瓦扩张) and ...

Example

The situation is completely different for the complex numbers $\mathbb{C}$. Consider, e.g. complex conjugation $^{-}: \mathbb{C} \to \mathbb{C} : a + b\mathrm{i} \mapsto a - b\mathrm{i}$ for $a, b \in \mathbb{R}$. It is easy to verify that this is a ring homomorphism. Obviously complex conjugation is not the identity on $\mathbb{C}$.

Proposition

Given the splitting field $F \subset E$ of an irreducible separable polynomial $p \in F[x]$ of degree n. Then $\mathrm{Aut}_F(E)$ is a transitive subgroup of S_n.

Galois extensions (伽罗瓦扩张) and ...II

Proof.

Obviously automorphisms of E are fixed by specifying the image of all the roots $\xi \in E$ of p. But due to the automorphism property these can only be mapped to other roots of p. Since p is separable it has exactly $n = \deg p$ different roots and any automorphism must thus be a permutation of these roots. This implies $\mathrm{Aut}_F(E) \subset S_n$. Let now ξ_1 be one of the roots and ξ_2 another one. Consider the extension $K := F(\xi_1, \xi_2)$ obviously $F \subset K \subset E$. Since each is finite dimensional, they are both algebraic extensions. Since ξ_i have both the same minimal polynomial p, we can construct an automorphism $\mathrm{Aut}_F(K) \ni \sigma : \xi_1 \mapsto \xi_2$. We can extend this automorphism from K to E and thus obtain an automorphism $\tilde{\sigma} \in \mathrm{Aut}_F(E)$ that maps ξ_1 to ξ_2, for every pair of roots ξ_k of p. This completes the proof. □

Galois extensions (伽罗瓦扩张) and ...III

Warning: This does not imply that the automorphism group is S_n, but rather a transitive subgroup, e.g. C_n, A_n (for $n \geq 3$), D_n (for $n \geq 3$), or S_n.

Definition

A field extension $F \subset E$ is called Galois (伽罗瓦的) *if it is separable and normal.*
The Galois group of an algebraic extension $F \subset E$ is $\mathrm{Gal}(E : F) := \mathrm{Aut}_F(E)$ *the set of all automorphisms of E that leave F invariant.*

Galois extensions (伽罗瓦扩张) and ...IV

Remark

Remember the definition of separability degree of an (algebraic) extension $F \subset E$ as the number of F-homomorphisms of E into $\bar{F}$. If E/F is normal (as in a Galois extension), then each such homomorphism sends E to itself, thus $|\operatorname{Aut}_F(E)| = [E : F]_s$. If moreover E is separable over F, then $[E : F]_s = [E : F]$. In total we obtain $|\operatorname{Gal}(E : F)| = [E : F]$.

The importance of Galois extensions comes from the following correspondence principle first discovered by Galois.[1]

[1] Évariste Galois *10/1811 in Bourg-la-Reine/France, †5/1832 in a duel (with guns) presumably about love but under rather dubious circumstances. Fortunately he wrote down his genial ideas before he entered the duel.

The correspondence principle

Theorem

Given a Galois extension $F \subset E$, then there is a 1:1-correspondence between intermediate fields $F \subset K \subset E$ and subgroups $H \subset \mathrm{Gal}(E : F)$, via

$$H \mapsto E^H := \{\alpha \in E : \forall \sigma \in H : \sigma(\alpha) = \alpha\}, \tag{1}$$

$$K \mapsto \mathrm{Gal}(E : K) \tag{2}$$

Moreover, Galois extensions $F \subset K$ with $K \subset E$ correspond to normal subgroups $H \triangleleft \mathrm{Gal}(E : F)$ and $\mathrm{Gal}(K : F) \cong \mathrm{Gal}(E : F)/\mathrm{Gal}(E : K)$.

The correspondence principle

Proof.

From Proposition 3.3.7 and Lemma3.5.4 it follows that E/K is always a Galois extension. Note that E^H is a ring, because the elements of $\mathrm{Gal}(E:F)$ are ring automorphisms. Also E^H contains the inverses for the same reason. Therefore E^H is a field and also contains F.

Let us verify that the operations are inverse to each other. Consider thus $k := E^{\mathrm{Gal}(E:K)}$. Obviously $K \subset k$. Assume there were an $\alpha \in k \setminus K$. But then there is an automorphism $\sigma \in \mathrm{Gal}(E:K)$ such that $\sigma(\alpha) \neq \alpha$, because α is F-linear independent from K. This would contradict k is $\mathrm{Gal}(E:K)$-invariant and therefore $k = K$.

Conversely let $H' := \mathrm{Gal}(E:E^H)$. Clearly $H \subset H'$. But by Remark 3.6.4 we also have $|H| = [E:E^H] = |H'|$ both finite, so $H = H'$.

The correspondence principle

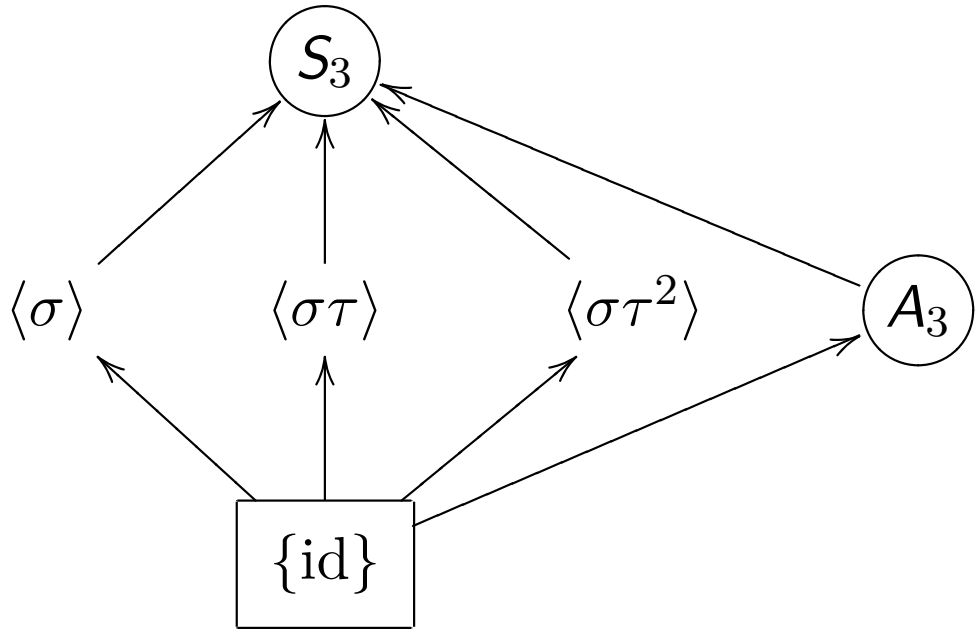
It remains to show that Galois extensions correspond to normal subgroups. Let thus $H \lhd G := \mathrm{Gal}(E/F)$ be a normal subgroup. As shown so far it corresponds to an intermediate field $F \subset E^H \subset E$. We also know that H is its own conjugate in G. That implies that $K := E^H$ is its own conjugate under all $\sigma \in G = \mathrm{Gal}(E : F)$. But then K/F is normal. This completes the proof. □

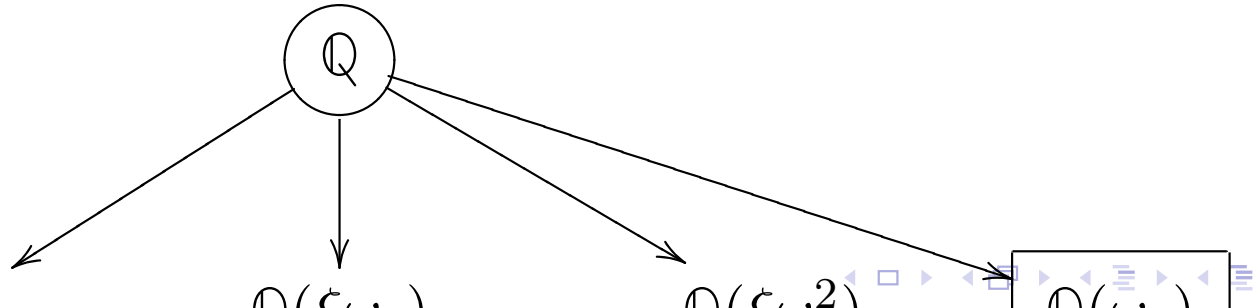
Example

Consider the extension $\mathbb{Q} \subset E := E_p$, the splitting field of $p = x^3 - 2 \in \mathbb{Q}[x]$. Beside $\xi = \sqrt[3]{2}$ is also contains the element $\omega_3 = \mathrm{e}^{2\pi \mathrm{i}/3}$ a third root of unity. Since the Galois group permutes the three solutions $\xi\omega_3^k$ of $p = x^3 - 2 \in \mathbb{Q}[x]$, it is a transitive subgroup of S_3, i.e. either A_3 or S_3 itself. Moreover the map $\sigma : E \to E : \xi \mapsto \xi, \omega_3 \mapsto \omega_3^{-1}$ is an automorphism of order 2 of E.

The correspondence principle III

Therefore $\mathrm{Gal}(p/\mathbb{Q}) = S_3$. The subgroups are $\{1, \langle\sigma\rangle, \langle\sigma\tau\rangle, \langle\sigma\tau^2\rangle, A_3, S_3\}$ and the corresponding fields $\{E, \mathbb{Q}(\xi), \mathbb{Q}(\xi\omega_3), \mathbb{Q}(\xi\omega_3^2), \mathbb{Q}(\omega_3), \mathbb{Q}\}$ and fit into the pattern:





The correspondence principle IV

The last statement in the Galois correspondence is very similar to the Second Isomorphism Theorem (for groups). So one may wonder if there is any (non-trivial) correspondence to the Third Isomorphism Theorem. The answer is the following:

Proposition

Given a finite Galois extension $F \subset E$ together with any field extension $F \subset K \subset L$ and also $E \subset L$, then the composite $EK \subset L$ exists, is Galois over K, as well as E is a finite Galois extension over $E \cap K$, and $\mathrm{Gal}(EK : K) \cong \mathrm{Gal}(E : (E \cap K))$.

The correspondence principle V

Proof.

Since E is normal over F, it is also normal over $F \subset E \cap K$, and thus every K-automorphism of EK has a restriction to E which is an $E \cap K$-automorphism. This yields a group homomorphism $\Theta\colon \operatorname{Gal}(EK : K) \to \operatorname{Gal}(E : (E \cap K)) : \sigma \mapsto \sigma|_E$. Since EK is generated by $E \cup K$, an F-homomorphism of EK is uniquely determined by its restrictions to E and to K. Therefore Θ is injective.

If $\alpha \in E$, then $(\sigma|_E)(\alpha) = \alpha$ for all $\sigma \in \operatorname{Gal}(EK : K)$ if and only if $\sigma\alpha = \alpha$ for all $\sigma \in \operatorname{Gal}(EK : K)$, if and only if $\alpha \in K$. Thus $E \cap K$ is the fixed field of $\operatorname{im}\Theta \subset \operatorname{Gal}(E : (E \cap K))$. But then Θ must be surjective and thus an isomorphism. □

Galois group of polynomials of low degree I

We denote $\mathrm{Gal}(p/F)$ the Galois group of the splitting field E_p of a separable polynomial $p \in F[x]$. In this way the Galois theory decides about the structure of the roots of a polynomial p.

Example

2. A monic quadratic polynomial $p = x^2 + px + q \in F[x]$ over a field not of characteristic 2 is irreducible iff $D_p := p^2 - 4q$ is not a square in F. In this case the Galois group is $C_2 \cong S_2$.

Note also that the Galois group of two polynomials $p_1 p_2$ that do not have roots in common $\gcd(p_1, p_2) \in F^*$ is $\mathrm{Gal}(p_1 p_2/F) = \mathrm{Gal}(p_1/F) \times \mathrm{Gal}(p_2/F)$.

Galois group of polynomials of low degree II

Remember the definition of the discriminant of a polynomial $p \in F[x]$ of degree n with roots $\alpha_1, \ldots, \alpha_n \in \bar{F}$ as follows

$$D_p := \prod_{i<j} (\alpha_i - \alpha_j)^2.$$

Since the discriminant is symmetric in all roots, it is a polynomial in its symmetric functions, the coefficients of the polynomial. Therefore $D_p \in F$.
In general the discriminant tells us the following about the Galois group:

Proposition

Given a separable polynomial $p \in F[x]$, then the Galois group $\mathrm{Gal}(p/F)$ *has an odd permutation iff its discriminant is not a square in F.*

Galois group of polynomials of low degree III

Proof.

The element $t := \prod_{i<j}(\alpha_i - \alpha_j)$ in any specific order of the roots of p is an element of the splitting field E_p of p. Moreover $D_p = t^2$ and so $t \in F(t)$ an extension of degree 1 or 2. Given any homomorphism $\sigma \in \mathrm{Gal}(p/F)$ of E_p into $\bar{F}$, then it maps $t \to \pm t$ depending on its sign in S_n. If $t \in F$, i.e. D_p has a square root in F, then no permutation can change the sign of t and so $\mathrm{Gal}(p/F) \subset A_n$. Conversely if there is any odd permutation in $\mathrm{Gal}(p/F)$, then t changes sign under this permutation and can thus not be an element of F. □

Galois group of polynomials of low degree IV

In degree 3 we get the following result:

Proposition

Given a monic polynomial of degree 3, $p = x^3 + px + q \in F[x]$ in reduced form over a field not of characteristic 2 or 3, then the Galois group $\mathrm{Gal}(p/F)$ *is*

- S_3 *iff the discriminant is not a square in F and p irreducible, thus* $[E_p : F] = 6$;
- A_3 *iff the discriminant is a square, but p irreducible and thus* $[E_p : F] = 3$;
- $\subset C_2$ *iff p is reducible.*

Galois group of polynomials of low degree V

In degree 4 the result is more involved and reads

Proposition

Let $p = x^4 + rx^2 + sx + t \in F[x]$ be a separable quartic polynomial in reduced form over a field not of characteristic 2. Then the order of the splitting field K of its resolvent divides 6. The Galois group of p is correspondingly

- S_4 *iff* $[K : F] = 6$ *and p irreducible;*
- A_4 *iff* $[K : F] = 3$ *and p irreducible;*
- D_4 *iff p is irreducible and* $[K : F] = 2$*;*
- C_4 *iff* $[K : F] = 2$ *and p irreducible (over F), but not irreducible over K;*
- V_4 *iff* $[K : F] = 1$ *(i.e. the resultant splits into linear factors over F) and p irreducible;*

$\subset S_3$ or $\subset C_2 \times C_2$ *(not transitive) iff p is reducible.*

Galois group of polynomials of low degree VI

The Galois groups depends importantly on the irreducibility (or the irreducible factors in general).

Exercises

Exercise

Let $F \subset E$ be a finite Galois extension and consider intermediate fields $F \subset K_i \subset E$ as well as corresponding subgroups $H_i \subset \mathrm{Gal}(E : F)$. Prove the following:

a. $K_1 \subset K_2$ iff $H_1 \supset H_2$;

b. $K_1 = K_2 K_3$ iff $H_1 = H_2 \cap H_3$;

c. $K_1 = K_2 \cap K_3$ iff $H_1 = \langle H_2, H_3 \rangle_{\mathrm{Gal}}$.

Exercise (Galois connection)

Given two partially ordered sets $(X, \leq)$ and $(Y, \leq)$ together with order reversing maps $F\colon X \to Y$ and $G\colon Y \to X$, i.e. for all $x_i \in X$ with $x_1 \leq x_2$ then $F(x_2) \leq F(x_1)$ and for all $y_i \in Y$ with $y_1 \leq y_2$ we have $G(y_2) \leq G(y_1)$. Show that F and G induce mutually inverse order-reversing bijections between $X^{GF} := \{x \in X : (GF)(x) = x\}$ and $Y^{FG} := \{y \in Y : (FG)(y) = y\}$.

Remark

The pair (F, G) is called a Galois connection between X and Y.

Exercise

Let $p = x^3 + x - 1 \in \mathbb{Q}[x]$ and compute its Galois group together with all intermediate fields between $\mathbb{Q}$ and the splitting field E of p. Which are Galois extensions over $\mathbb{Q}$?

Exercise

Compute the Galois groups of the following polynomials

a. $x^3 - x - 1$ over $\mathbb{Q}(\sqrt{-23})$,

b. $x^3 - 10 \in \mathbb{Q}[x]$,

c. $x^3 - 10$ over $\mathbb{Q}(\sqrt{2})$,

d. $x^3 - 10$ over $\mathbb{Q}(\sqrt{-3})$,

e. $(x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$,

f. $x^4 - 3 \in \mathbb{Q}[x]$

g. $x^4 - 3$ over $\mathbb{Q}(\sqrt{3})$,

h. $x^4 - 3$ over $\mathbb{Q}(\sqrt{-3})$,

i. $x^4 + x + 3 \in \mathbb{Q}[x]$,

j. $x^4 + 3x + 3 \in \mathbb{Q}[x]$.