Legend: Everything in *green* is from the Bergman's Companion to Lang's Algebra.

In this chapter we will study the core of Galois theory, the group of automorphisms of a finite (and sometimes infinite) Galois extension at length.

1 Galois extensions

Definition 1. Let K be a field and let G be a group of automorphisms of K. We let

$$K^G = \{x \in K \mid x^\sigma = x \text{ for all } \sigma \in G\}$$

We call this the **fixed field** of G.

Definition 2. An algebraic extension K of a field k is called **Galois** if it is normal and seperable.

The group of automorphisms of K over k is called the **Galois group** of K over k, and is denoted $G(K/k)$, $G_{K/k}$, $\mathrm{Gal}(K/k)$ or simply G.

This is the main theorem of the Galois theory or finite Galois extensions.

Theorem 1. Let K be a finite Galois extension of k, with Galois group G. There is a bijection between the set of subfields E of K, containing k and the set of subgroups H of G, given by $E = K^H$. The field E is Galois over k if and only if H is normal in G, and if that is the case, then the map $\sigma \to \sigma|_E$ induces an isomorphism of G/H onto the Galois group of E over k.

Theorem 2. Let K be a Galois extension of k. Let G be its Galois group. Then $k = K^G$. If F is an intermediate field, $k \subseteq F \subseteq K$, then K is Galois over F. The map

$$F \to \mathrm{Gal}(K/F)$$

from the set of intermediate fields into the set of subgroups of G is injective.

Proof. Let $\alpha \in K^G$. Let σ be any embedding of $k(\alpha)$ in K^a, inducing the identity on k. Extend σ to an embedding of K into K^a, we also call this extension σ. Note since K is normal, σ is an automorphisms of K over k it is an element of G. Since $\alpha \in K^G$, σ leaves α fixed. Therefore there is actually only one extension of σ to an embedding of K in K^a (the identity). So:

$$[k(\alpha)\colon k]_s = 1$$

Since α is seperable over k, $[k(\alpha)\colon k] = [k(\alpha)\colon k]_s = 1$, so $\alpha \in k$. This proves the first assertion.

Let F be an intermediate field. Then K is normal and seperable over F by previous theorems from chapter five. Hence K is Galois over F. If $H = \mathrm{Gal}(K/F)$ then by what we have proved above we conclude that $F = K^H$. Now we will show that the map defined in our statement is injective. Let F, F' be intermediate fields such that $F \to \mathrm{Gal}(K/F) = H$ and $F' \to \mathrm{Gal}(K/F') = H'$.

Assume that $H = H'$, then:

$$F = K^H = K^{H'} = F'$$

□

Definition 3. We shall call the group $\mathrm{Gal}(K/F)$ of an intermediate field the group **associated** with F. We say that a subgroup H of G **belongs** to an intermediate field F if $H = \mathrm{Gal}(K/F)$

Bergman 1. *Note this does not mean that H is the Galois group of F. For example the Galois group of the whole extension K is $Gal(K/F)$, $\{1\}$ is the subgroup belonging to K, since $\{1\} = Gal(()K/K)$.*

Corollary. Let K/k be Galois with group G. Let F, F' be two intermediate fields, and let H, H' be the subgroups of G belonging to F, F' respectively. Then $H \cap H'$ belongs to FF'.

Proof. Note every element of $H \cap H'$ leaves FF' fixed (basically from how FF' is constructed), and every element of G

which also leaves FF' fixed also leaves F and F' fixed so lies in $H \cap H'$. □

Corollary. The fixed field of the smallest subgroup of G containing H and H' is $F \cap F'$.

Proof. Let E be the smallest subgroup of G containing H and H'. Note this means that $E = \langle H \cup H' \rangle$.

Let $x \in K^E$. This means that

$$\sigma(x) = x \text{ for all } \sigma \in E$$

Since $H, H' \subseteq E$ we see that $x \in K^H = F$ and $x \in K^{H'} = F'$. So $x \in F \cap F'$. On the other hand, if $x \in F \cap F'$, then for $\sigma \in E$ we have $\sigma = \tau_1 \cdots \tau_n$, where $\tau_i \in H \cup H'$.

So

$$\sigma(x) = \tau_1 \circ \cdots \circ \tau_{n-1} \circ \tau_n(x) = \tau_1 \circ \cdots \circ \tau_{n-1}(x) = \ldots = x$$

Since $\tau_i(x) = x$ for all i,

Therefore we indeed see that $F \cap F' = K^E$. □

Corollary. $F \subseteq F'$ if and only if $H' \subseteq H$

Proof. If $F \subseteq F'$ and $\sigma \in H'$ leaves F' fixed, then σ leaves F fixed, so $\sigma \in H$. So $H' \subseteq H$.

Conversely if $H' \subseteq H$, then $F = K^H \subseteq K^{H'} = F'$. □

Corollary. Let E be a finite seperable extension of a field k. Let K be the smallest normal extension of k containing E. Then K is finite Galois over k. There is only a finite number of intermediate fields F such that $k \subseteq F \subseteq E$.

Proof. Note K is the compositum of a the finite number of conjugates of E, i.e

$$K = (\sigma_1 E) \cdots (\sigma_n E) \text{ where } \sigma_i \text{ are the distinct embeddings of } E \text{ into } E^a$$

Therefore it is normal(by definition), seperable(since E is) and it is finite over k.

The Galois group K/k has only a finite number of subgroups. So there is only a finite number of subfields of K containing k, so a finite number of subfields of E containing k. □

Lemma 1. Let E be an algebraic seperable extension of k. Assume that there is an integer $n \geq 1$ such that every element $\alpha \in E$ is of degree $\leq n$ over k. Then E is finite over k and $[E\colon k] \leq n$.

Proof. Let $\alpha \in E$ be such that $m = [k(\alpha)\colon k] \leq n$ is maximal. Assume that, there exists $\beta \in E \setminus k(\alpha)$, then since $k(\alpha, \beta)$ is seperable and finite over k by the primitive element theorem there is a $\gamma \in k(\alpha, \beta) \subseteq E$ such that:

$$[k(\gamma)\colon k] = [k(\alpha, \beta)\colon k] > m$$

Which contradicts our assumption that α had maximal degree in E. Therefore $E \setminus k(\alpha) = \emptyset \Rightarrow E = k(\alpha)$,

So it is finite over k and $[E\colon k] \leq n$. □

Theorem 3. **Artin** Let K be a field and let G be a finite group of automorphisms of K, of order n. Let $k = K^G$ be the fixed field. Then K is a finite Galois extension of k, and its Galois group is G. We have $[K\colon k] = n$,

Proof. Let $\alpha \in K$ and let $\sigma_1, \ldots, \sigma_r$ be a maximal set of elements of G such that $\sigma_1\alpha, \ldots, \sigma_r\alpha$ are distinct. If $\tau \in G$ then for all i, there is a $\xi \in S_r$ such that

$$\tau\sigma_i\alpha = \sigma_{\xi(i)}\alpha$$

Indeed $\tau\sigma_i\alpha \in \{\sigma_1\alpha, \ldots, \sigma_r\alpha\}$, by maximality. And since τ is injective, $\tau\sigma_i\alpha = \tau\sigma_j\alpha \iff \sigma_i\alpha = \sigma_j\alpha$.

So not only is α the root of a polynomial

$$f(X) = \prod_{i=1}^{r}(X - \sigma_i\alpha) \text{ and } \forall \tau \in G,\ f^\tau = f$$

So the coefficients of f are in $K^G = k$. Furthermore, f is seperable since all the $\sigma_i\alpha$ are distinct. So every element $\alpha \in K$ is the root of a seperable polynomial of degree $\leq n$ with coeffs in k. We also see that this polynomial splits into

linear factors in K, so K is seperable and normal (hence Galois) over k.

By lemma 3 we see that $[K\colon k] \leq n$. But recall from chapter 5, the Galois group of K over k has order $\leq [K\colon k]$. Since $G \subseteq \mathrm{Gal}(()K/k)$, but $n = |G| \leq |\mathrm{Gal}(()K/k)| \leq [K\colon k] \leq n$, we see that $G = \mathrm{Gal}(()K/k)$, and $[K\colon k] = n$. □

Corollary. Let K be a finite Galois extension of k and let G be its Galois groiup. Then every subgroup of G belongs to some subfield F such that $k \subseteq F \subseteq K$.

Proof. Let $H \leq G$, and $F = K^H$, then by Artin K is a finite Galois extension of F and $\mathrm{Gal}(K/F) = H$. □

Bergman 2. *Combining this corollary and theorem 2, tells us that we have a bijection between the set of subfields of K containing k and the set of subgroups of G. i.e, the first assertion in theorem 1*

This is called the ***Fundamental Theorem of Galois Theory***

Remark. This only covers the finite case, if K is an infinite Galois extension of k we need to do more work.

Let K be a Galois extension of k. Let

$$\lambda\colon K \to \lambda K \text{ be an isomorphism}$$

Then λK is a Galois extension of λk. Let G be the Galois groupnof K over k. Then the map

$$\sigma \to \lambda\sigma\lambda^{-1}$$

Gives a homomorphism of G into $\mathrm{Gal}(\lambda K/\lambda k)$. Furthermore this homomorphism has an iverse given by

$$\lambda^{-1}\tau\lambda \to \tau$$

Therefore these two groups are isomorphic and we write:

$$G(\lambda K/\lambda k)^{\lambda} = G(K/k) \text{ or } G(\lambda K/\lambda k) = \lambda G(K/k)\lambda^{-1}$$

Where λ is "conjugation" such that

$$\sigma^{\lambda} = \lambda^{-1}\sigma\lambda \text{ where we have the property} (\sigma^{\lambda})^{\omega} = \sigma^{\lambda\omega}$$

Bergman 3. *Note we may write ${}^{\lambda}\sigma = \lambda\sigma\lambda^{-1}$, and then ${}^{\lambda}({}^{\omega}\sigma) = \lambda({}^{\omega}\sigma)\lambda^{-1} = \lambda\omega\sigma\omega^{-1}\lambda^{-1} = {}^{\lambda\omega}\sigma$*

In particular, let F be an intermediate field, $k \subseteq F \subseteq K$, and let $\lambda\colon F \to \lambda F$ be an embedding of F in K, which we extend to an automorphisms of K. Then $\lambda K = K$ and

$$\mathrm{Gal}(K/\lambda F)^{\lambda} = \mathrm{Gal}(K/F)$$

Theorem 4. Let K be a Galois extension of k with group G. Let F be a subfield, $k \subseteq F \subseteq K$ and let $H = \mathrm{Gal}(K/F)$. Then F is normal over k if and only if H is normal in G.

If F is normal over k, then the restriction map $\sigma \to \sigma|_F$ is a homomorphism of G onto the Galois group of F over k, whose kernel is H. We thus have

$$\mathrm{Gal}(F/k) \simeq G/H$$

Proof. Assume F is normal over k, and let G' be its Galois group. The restriction map $\sigma \to \sigma|_F$ maps G into G'. By definition its kernel is H.

Since F is normal over k, we know that $\sigma|_F\colon F \to F$, so this map is a homomorphism so H is the kernel of a hom, so it is normal in G.

Furthermore, any element $\tau \in G'$ extends to an embedding of K in K^a, which must be an automorphism of K (since K is normal) so the restriction map is surjective. So we indeed see that

$$G/H \simeq \mathrm{Gal}(F/k)$$

Now assume that F is not normal over k. There exists an embedding λ of F in K over k which is not an automorphism, i.e. $\lambda F \neq F$. Extend λ to an automorphism of K over k. The Galois groups $G(K/\lambda F)$ and $G(K/F)$ are conjugate, and they belong to distinct subfields, hence cannot be equal. So H is not normal in G. □

Remark. The above theorem says that if $H \trianglelefteq G$, then F is Galois over k. Indeed, since K is Galois over F and Galois over k we have:

$$|G| = [K\colon k] = [K\colon F][F\colon k] = |H|[F\colon k]$$

Recall we are considering finite extensions in this section, so

$$\begin{aligned}[F\colon k] &= |G/H| \\ &= |\mathrm{Gal}(F/k)| \\ &= [F\colon k]_s\end{aligned}$$

The last equality is true since F/k is a normal extension. So F/k is normal and seperable, so it is a Galois extension.

Definition 4. A Galois extension K/k is said to be **aberlian** (resp. **cyclic**) if its Galois group G is Abelian (resp. cyclic).

Corollary. Let K/k be abelian (resp. cyclic). If F is an intermediate field, $k \subseteq F \subseteq K$, then F is Galois over k and is abelian (resp. cyclic).

Proof. Let $G(K/F) = H \leq G$, since G is abelian then H is also and so is normal in G. So F is Galois over k, and G/H is abelian since the quotient of abelian groups is abelian.

We replace the word *abelian* with *cyclic* for the proof about cyclic extensions. □

Theorem 5. *Theorem of Natural Irrationalities*
Let K be a Galois extension of k, and let F be an arbitrary extension. Assume that K, F are subfields of some other field. Then KF is Galois over F, and K is Galois over $K \cap F$. Let H be the Galois group of KF over F, and G the Galois group of K over k. If $\sigma \in H$ then the restriction of σ to K is in G and the map

$$\sigma \to \sigma|_K$$

gives an isomorphism of H on the Galois group of K over $K \cap F$.

Note KF is Galois over F since seperable extensions form a distinguised class of extensions, so KF/F is seperable, and normal extensions remain normal under lifting so KF/F is normal.

Also $k \subseteq K \cap F \subseteq K$, so K is Galois over $K \cap F$.

Now let $\sigma \in H$. The restriction of σ to K is an embedding of K over k, so is an element of G since K is normal over k. So again the map $\sigma \to \sigma|_K$ is an homomorphism. If $\sigma|_K$ is the identity, then σ must be the identity of KF (since every element of KF can be expressed as a combination of sums and products and quotients of elements in K and F, and since σ is in the Galois group of KF over F, it also fixes F).

So our homomorphism $\sigma \to \sigma|_K$ is injective. Let H' be its image. Then H' leaves $K \cap F$ fixed. Conversely, if an element $\alpha \in K$ is fixed under H', we see that α is also fixed under H so $\alpha \in F$ and $\alpha \in K \cap F$. So $K \cap F$ is the fixed field.

If K is finite over k, or KF is finite over F, then by theorem 4, H' is the Galois group of K over $K \cap F$. □

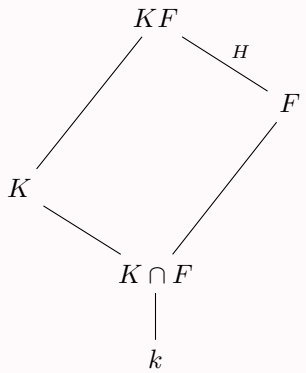


Diagram illustrating the theorem

It is suggestive to think of the opposite sides of the parallelogram as being equal, under the particular hypotheses of the preceding theorem.

Bergman 4. *The preceding theorem basically says that if one of the lower edges of the parallelogram is a Galois extension then the parallel upper edge is also Galois, with the same Galois group.*

Corollary. Let K be a finite Galois extension of k. Let F be an arbitrary extension of k. Then $[KF\colon F]$ divides $[K\colon k]$.

Proof. In the notation from above, the order of H divides the order of G, since $\mathrm{Gal}(K/K\cap F)$ is a subgroup of $\mathrm{Gal}(K/k)$. The result follows. □

Remark. WARNING The assertion of the corollary is not usually valid if K is not Galois over k.

Let $\alpha = \sqrt[3]{2}$ be the real cube root of 2, and let ζ be a primitive third root of unity, say

$$\zeta = \frac{-1+\sqrt{-3}}{2}$$

and let $\beta = \zeta\alpha$. Let $K = \mathbb{Q}(\beta)$ and $F = \mathbb{Q}(\alpha)$, since $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$ we see that $\mathbb{Q}(\beta) \neq \mathbb{Q}(\alpha)$.

So $K \cap F$ is a subfield of K whose degree over $\mathbb{Q}$ divides 3, since $3 = [F\colon \mathbb{Q}] = [F\colon K\cap F][K\cap F\colon \mathbb{Q}]$ and $2 = [K\colon \mathbb{Q}] = [K\colon E\cap F][K\cap F\colon \mathbb{Q}]$, so

$$[K\cap F\colon \mathbb{Q}] = 1$$

But $KF = \mathbb{Q}(\alpha,\beta) = \mathbb{Q}(\alpha,\sqrt{-3})$, so $[KF\colon F] = 2$.

Bergman 5. *If we look back at our diagram, this example shows is that even the equality of degrees between the opposite sides can fail if the lower edge is not normal. Moreover, each upper edge of the parallelogram is an extension of degree 2, and every quadratic extension is normal. So the top two edges are normal, but the opposite edges are not in any sense "equal".*

Theorem 6. Let K_1 and K_2 be Galois extensions of a field k, with Galois groups G_1 and G_2 respectively. Assume K_1, K_2 are subfields of some field. Then K_1K_2 is Galois over k. Let G be its Galois group. Map $G \to G_1 \times G_2$ by restriction:

$$\sigma \mapsto (\sigma|_{K_1}, \sigma|_{K_2})$$

The map is injective, if $K_1 \cap K_2 = k$ then the map is an isomorphism.

Proof. K_1K_2 is Galois over k since normality and seperability are preserved by compositum. Furthermore our map is clearly and homomorphism of G into $G_1 \times G_2$. If $\sigma \in G$ induces the identity on K_1 and K_2 then it induces the identity on their compositum so our map is injective. Assume that $K_1 \cap K_2 = k$ then by theorem 6, given an element $\sigma \in G_1$ there is an element σ of the Galois group K_1K_2 over K_2, which induces σ_1 on K_1.

This σ is in G and induces the identity on K_2. Hence $G_1 \times \{e_2\}$ is contained in the image of our homomorphism. Similarly for $\{e_1\} \times G_2$. Hence their product, $G_1 \times G_2$, is contained in the image. □

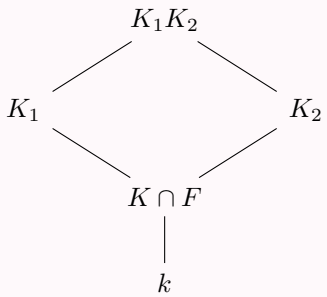


Diagram illustrating the theorem

Corollary. Let $K_1, \ldots, K_n$ be Galois extensions of k with Galois groups $G_1, \ldots, G_n$. Assume that $K_{i+1} \cap (K_1 \cdots K_i) = k$ for each $i = 1, \ldots, n-1$. Then the Galois group of $K_1 \cdots K_n$ is isomorphic to the product $G_1 \times \cdots \times G_n$ in the natural way.

Proof. Induction, using the previous theorem. □

Corollary. Let K be a finite Galois extension of k with group G, and assume that G can be written as a direct product

$$G = G_1 \times \cdots \times G_n$$

Let K_i be the fixed field of

$$G_1 \times \cdots \times G_{i-1} \times \{1\} \times G_{i+1} \times \cdots \times G_n$$

Then K_i is Galois over k and $K_{i+1} \cap (K_1 \cdots K_i) = k$. Furthermore $K = K_1 \cdots K_n$

Proof. Recall the compositum of all K_i belongs to the intersection of their corresponding groups, which is the identity. Hence the compositum is equal to K. Each factor of G is normal in G, so K_i is Galois over k. Recall the intersection of normal extensions belongs to the product of their Galois groups. And it is clear that

$$K_{i+1} \cap (K_1 \cdots K_i) = k$$

□

Theorem 7. Assume all fields are contained in some common field.

1. If K, L are abelian over k, so is the composite KL.
2. If K is abelian over k and E is any extension of k, then KE is abelian over E.
3. If K is abelian over k and $K \supseteq E \supseteq k$, where E is an intermediate field, then E is abelian over k and K is abelian over E

Proof. Immidiate theorem 6 and theorem 7 □

Definition 5. If k is a field, the composite of all abelian extensions of k in a given algebraic closure k^a is called the **maximum abelian extension** of k and is denoted k^{ab}.

Bergman 6. *Lang calls the notations of k^a, k^s and k^{ab} "functiorial with respect to the ideas". It was one of his slogans. He may be saying that the notation should reflect ideas in something like the way the functiorial notation does (i.e. with functors we write $F(a)\colon F(X) \to F(Y)$, if $a\colon X \to Y$ induces a map $F(x) \to F(Y)$ instead of a^* as we would have in the pre-category theory days). The use of k^a, k^s and k^{ab} rather than arbitrary bars and tildas does this.*

Galois connections

Bergman 7. *The FTG is an example of a general type of mathematical situation*

Definition 6. Let S, T be sets and $R \subseteq S \times T$ be a binary relation on them. For every subset $X \subseteq S$ we define

$$X^* = \{t \in T \mid (\forall s \in X),\ (s,t) \in R\} \subseteq T$$

And likewise for every subset $Y \subseteq T$ we define

$$Y^* = \{s \in S \mid (\forall t \in Y),\ (s,t) \in R\} \subseteq S$$

These operators constitute what is called the **Galois connection** between S and T.

So note in our case, S is an extension field K of k, $T = Gal(K/k)$ and R is the relation

$$\{(x, \sigma) \in K \times Gal(K/k) \mid \sigma(x) = x\}$$

$X \subseteq X' \Rightarrow X^* \supseteq X'^*$

The operators $**$ from $P(S) \to P(S)$ and $P(T) \to P(T)$, are the closure operators on S and T, i.e.

- $X \subseteq X^{**}$
- $X \subseteq Y \Rightarrow X^{**} \subseteq Y^{**}$
- $(X^{**})^{**} = X^{**}$

The operators $*$ give a bujective inclusion-reversing correspondence between closed subsets of S and closed subsets of T wrt to these operators.

2 Examples and Applications

Bergman 8. *Let K be a finite field, say $\mathbb{F}_{p^n}$, recall the Frobenius map is an automorphism in this case, furthermore we recall that this map fixes $\mathbb{F}_p$. Furthermore the Frobenius map has finite order, so by Artin it generates the group $Gal(\mathbb{F}_{p^n}/\mathbb{F}_p)$. Thus each field $\mathbb{F}_{p^n}$ is a Galois extension of $\mathbb{F}_p$ with cyclic Galois group, which must have order $[\mathbb{F}_{p^n}, \mathbb{F}_p] = n$.*

We can see that for every m dividing n, the sugroup generated by the mth power of the Frobenius map corresponds to a subfield $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$

Definition 7. Let k be a field and $f(X)$ a seperable polynomial of degree ≥ 1 in $k[X]$. Let

$$f(X) = (X - \alpha_1) \cdots (X - \alpha_n)$$

be its factorization in a splitting field K over k. If G is the Galois group of K over k, we call G the **Galois group** of f over k. Since the elements of G permute the roots of f, we have an injective homomorphism of G into the symmetric group S_n.

Quadratic extensions

Example 1. Let k be a field and $a \in k$. If a is not a square in k, then the polynomial $X^2 - a$ has no root in k and is therefore irreducible.

Assume $char k \neq 2$. Let α be a root, this polynomial is separable since $-\alpha \neq \alpha$, and so $k(\alpha)$ is the splitting field, is Galois and it's Galois group is cyclic of order 2.

Conversely, given an extension K of k of degree 2, there exists $a \in k$ such that $K = k(\alpha)$ and $\alpha^2 = a$. (Indeed since if $x^2 + bx + c = 0 \Rightarrow (x + \frac{b}{2})^2 = -(\frac{b^2}{4} + c) \in k$, so we let $\alpha = x + \frac{b}{2}$)

Bergman 9. *Recall that D and δ are the polynomials*

$$\delta(t) = \prod_{i<j}(t_i - t_j)$$
$$D = D(s_1, \ldots, s_n) = \prod_{i<j}(t_i - t_j)^2$$

Lemma 2. Let n be a positive integer, and let $D \in \mathbb{Z}[X_1, \ldots, X_n]$ be the discriminant polynomial. That is the unique polynomial such that in the polynomial ring $\mathbb{Z}[t_1, \ldots, t_n]$, if one writes s_i for the ith elementary symmetric polynomial in the t_i, we have

$$\prod_{i<j}(t_i - t_j)^2 = D(s_1, \ldots, s_n)$$

For any field k not of characteristic 2 and any seperable monic polynomial $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0$, if we denote by E the splitting field of f and by $\alpha_1, \ldots, \alpha_n$ the roots of f in E, then TFAE:

(a) Gal(E/k), regarded as a group of permutations of $\alpha_1, \ldots, \alpha_n$ lies in the alternating group A_n, i.e. acts by even permutations on these roots.

(b) The element $\delta(\alpha) = \prod_{i<j}(\alpha_i - \alpha_j)$ of E lies in k.

(c) The element $D(a_{n-1}, \ldots, a_0) \in k$ is asquare in k

Hence the fixed field of the group of elements of $\mathrm{Gal}(E/k)$ which act by even permutations on the roots of f is $k(\delta(\alpha)) = k(D(a_{n-1}, \ldots, a_0)^{1/2})$.

Proof. • $(a \Rightarrow b)$.

Let $\varphi_{(i,i+1)}$ be the automorphism of $\mathbb{Z}[t_1, \ldots, t_n]$ such that $\varphi_{(i,i+1)}(t_k) = t_{(i,i+1)k}$, where $(i, i+1)$ is a permutation. This automorphism takes $\delta(t) = \prod_{i<j}(t_i - t_j)$ to $-\delta(t)$. Since an odd permutation can be characterised as the product of an odd number of permutations of this form, and an even permutation is characterised by an even number of permutations of this form. We see that any odd permutation sends $\delta(t)$ to $-\delta(t)$ and any even permutation sends it to itself.

If an automorphism θ of E acts by a permutation π_θ on the roots $\alpha_1, \ldots, \alpha_n$ of f, then the map $\mathbb{Z}[t_1, \ldots, t_n] \to E$ carrying t_i to α_i makes a commuting square with the automorphism θ to the automorphism of the polynomial ring acting by π_θ on the subscripts of the indeterminates.

So θ will send $\delta(\alpha)$ to itself if π_θ is even and it's opposite if it is odd. Hence if all the members of $\mathrm{Gal}(E/K)$ act by even permutations on $\alpha_1, \ldots, \alpha_n$ then $\delta(\alpha)$ is fixed under that group. Hence belongs to k.

- $(b \Rightarrow a)$ Conversely, if $\delta(\alpha)$ belongs to k, then all memebers of the Galois group fix it, hence act by even permutations.
- $(b \Rightarrow c)$ Since $\delta(\alpha) \in k$ then $D(a_{n-1}, \ldots, a_0) = \delta(\alpha)^2 \in k$.
- $(c \Rightarrow b)$ Since $D(a_{n-1}, \ldots, a_0)$ is a square in k it has a root in k, but $X^2 - D(a_{n-1}, \ldots, a_0)$ can have at most two roots in E, it's only roots are $\pm\delta(\alpha)$ so $\delta(\alpha) \in k$.

□

Finally we note a final fact about the discriminant.

Lemma 3. Let n and D be as before, let k be any field and $f = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ be any monic polynomial of degree n over k. Then f is inseperable (has at least one multiple root in k^a) if and only if $D(a_{n-1}, \ldots, a_0) = 0$.

Proof. Let $\alpha_1, \ldots, \alpha_n$ be the roots of f then

$$\prod_{i<j}(\alpha_i - \alpha_j)^2 = D(a_{n-1}, \ldots, a_0) = 0 \iff \alpha_i = \alpha_j \text{ for some } 1 \le i < j \le n \iff f \text{ has a multiple root in } k^a$$

□

Cubic extensions

Example 2. Let k be a field not of characteristic 2 nor 3. Let

$$f(X) = X^3 + aX + b$$

Be any polynomial of degree 3 can be brought into this form (depressed cubic). Assume that f has no root in k. Then f is irreducible. Let α be a root of $f(X)$, Then $[k(\alpha) \colon k] = 3$.

Let K be the splitting field, since char $k \neq 2, 3$, f is separable, so let G be the Galois group. Then G has order 3 or 6 since G is a subgroup of the symmetric group S_3. In the second case $k(\alpha)$ is not normal over k, this is because the corresponding group is the stablizer of $1 \in \{1, 2, 3\}$ in S_3 which is not a normal subgroup.

How do we test whether the Galois group is the full symmmetric group? We will consider the discriminant, if $\alpha_1, \alpha_2, \alpha_3$ are the distinct roots of $f(X)$ we let

$$\delta = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_1 - \alpha_3) \text{ and } \Delta = \delta^2$$

If G is the Galois groups and $\sigma \in G$, then $\sigma(\delta) = \pm\delta$. Hence σ leaves Δ fixed. Thus Δ is in the ground field k. Furthermore we have seen that

$$\Delta = -4a^3 - 27b^2$$

The set of σ in G which leave δ fixed is precisely the set of even permutations. Thus G is the symmetric group if and only if Δ is not a square in k. We summarize this by saying:

Let $f(X)$ be a cubic polynomial in $k[X]$, and assume *char* $k \neq 2, 3$. Then

(a) f is irreducible over k if and only if f has no root in k.

(b) Assume f irreducible. The the Galois group of f is S_3 if and only if the discriminant of f ois not a square in k. If the discriminant is a square, then the Galois group is cuclic of order 3, equal to the alternating group A_3 as a permutation of the roots of f.

For instance, consider

$$f(X) = X^3 - X + 1$$

over the rational numbers. Any rational root must be 1 or -1, and so $f(X)$ is irreducible over $\mathbb{Q}$. The discriminant is -23 and is not a square. Hance the Galois group is the symmetric group. The splitting field contains a subfield of degree 2, namely $k(\delta) = k(\sqrt{\delta})$.

On the hand, let $f(X) = X^3 - 3X + 1$. Then f has no root in $\mathbb{Z}$, whence no root in $\mathbb{Q}$, so f is irreducible. The discriminant is 81, a square, so the Galois group is cyclic of order 3.

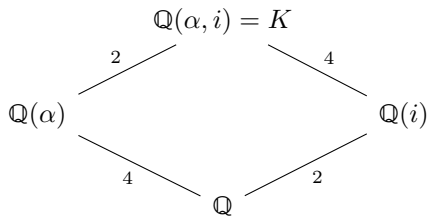
Example 3. We consider the polynomial $f(X) = X^4 - 2$ over the rationals $\mathbb{Q}$. It is irreducible by Eisenstein's criterion. Let α be a real root. Let $i = \sqrt{-1}$. Then $\pm\alpha$ and $\pm i\alpha$ are the four roots of $f(X)$, and

$$\mathbb{Q}(\alpha)\colon \mathbb{Q} = 4$$

Hence the splitting field of $f(X)$ is

$$K = \mathbb{Q}(\alpha, i)$$

Since α is real, $i \notin \mathbb{Q}(\alpha)$. But i satisfies the polynomial X^2+1, hence it has degree 2 over $\mathbb{Q}(\alpha)$ and therfore $[K\colon \mathbb{Q}] = 8$. So the Galois group of $f(X)$ has order 8. There exists an automorphism τ of K leaving $\mathbb{Q}(\alpha)$ fixed, sending i to $-i$, because K is Galois over $\mathbb{Q}(\alpha)$, of degree 2. Then $\tau^2 = id$.



By the multiplicativity of degrees in towers, we see that the degrees are as indicated in the diagram. Thus $X^4 - 2$ is irreducible over $\mathbb{Q}(i)$. Also, K is normal over $\mathbb{Q}(i)$. There exists an automorphism σ of K over $\mathbb{Q}(i)$ mapping the root α of $X^4 - 2$ to the root $i\alpha$.

Note that

$$\sigma^2(\alpha) = \sigma(i\alpha) = i\sigma(\alpha) = -\alpha.$$

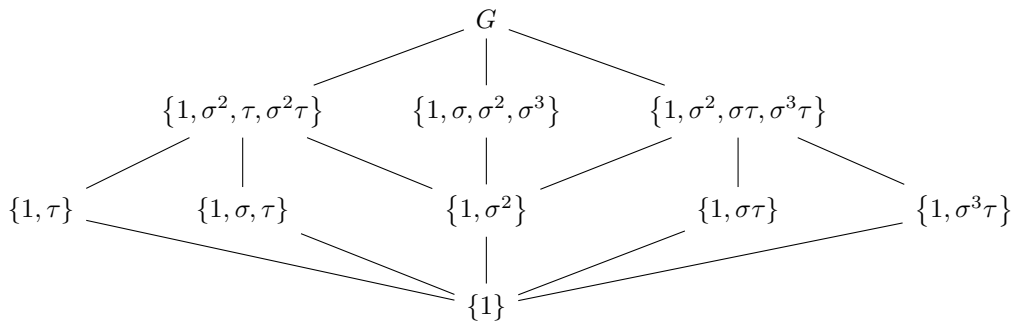
So $\sigma \neq \sigma^2$, likewise we see that $1, \sigma, \sigma^2, \sigma^3$ are distinct. Furthermore notice that $\sigma^4(\alpha) = i^4\alpha = \alpha$, from this we can conclude that $\sigma^4 = id$. Thus σ generates a cyclic group of order 4, denoted $\langle\sigma\rangle$. Since $\tau \in \langle\sigma\rangle$ it follows that $G = \langle\sigma, \tau\rangle$ is generated by σ and τ because $\langle\sigma\rangle$ has index 2. Furthermore, we can see that:

$$\tau\sigma(\alpha) = \tau(i\alpha) = -\alpha \text{ and } \sigma^3\tau(\alpha) = \sigma^3(\alpha) = i^3\alpha = -\alpha.$$

Likewise we have

$$\tau\sigma(i) = \tau(i) = -i \text{ and } \sigma^3\tau(i) = \sigma^3(-i) = -i.$$

From this we can conclude that $\tau\sigma = \sigma^3\tau$. This gives us a structure of G.



(1)

Bergman 10. *We can see that the four roots of $X^4 - 2$ in the complex plane form the vertices of a square, and the Galois group of this equation acts on these roots as the full symmetry group of the square.*

Example 4. Let k be a field and let $t_1, \ldots, t_n$ be algebraically independent over k. Let $K = k(t_1, \ldots, t_n)$. The symmetric group G on n letters operates on K by permuting $(t_1, \ldots, t_n)$ and its fixed field is the field of symmetric functions, by definition the field of those elements of K fixed under G. Let $s_1, \ldots, s_n$ be the elementary symmetric polynomials, and let

$$f(X) = \prod_{i=1}^{n} (X - t_i).$$

Up to a sign, the coeffiecients of f are $s_1, \ldots, s_n$. Letting $F = K^G$ we notice that since G fixes t_i we have

$$k(s_1, \ldots, s_n) \subseteq F.$$

Since F is the fixed field of a group of order $n!$, K has degree $n!$ over it. Hence it has degree at least $n!$ over $k(s_1, \ldots, s_n)$, with strict inequality if this field is strictly smaller than F. Since K is generated over that subfield by the roots of f, the degree of K over that subfield is also at most $n!$. Hence $F = k(s_1, \ldots, s_n)$.

Definition 8. The polynomial $f(X)$ above is called the **general polynomial of degree** n.

We have just constructed a Galois extension whose Galois group is the symmetric group.

The complex numbers are algebraically closed We will use the following properties of $\mathbb{R}$, it is an ordered field, every positive element is a square and every polynomial of odd degree in $\mathbb{R}[x]$ has a root in R. Let $i = \sqrt{-1}$ (a root of $X^2 + 1$). We claim that every element in $\mathbb{R}(i)$ has a square root, indeed if $a + bi \in \mathbb{R}(i)$, then the square root is given by $c + di$, where

$$c^2 = \frac{a + \sqrt{a^2 + b^2}}{2} \text{ and } d^2 = \frac{-a + \sqrt{a^2 + b^2}}{2}.$$

Since $\mathbb{R}$ has characteristic 0, every finite extension is seperable. Every finite extension of $\mathbb{R}(i)$ is contained in an extension K which is finite and Galois over $\mathbb{R}$. Let G be the Galois group over $\mathbb{R}$ and let H be a 2-Sylow subgroup of G. Let F be the fixed field. Counting degrees and orders, we find that the degree of F over $\mathbb{R}$ is odd. By the primitive element theorem, there exists and element $\alpha \in F$ such that $F = \mathbb{R}(\alpha)$. Then α is the root of an irreducible polynomial in $\mathbb{R}[x]$ of odd degree. This means that this degree is 1. Hence $G = H$ is a 2-group. Recall that K is Galois over $\mathbb{R}(i)$. Let G_1 be its Galois group. Since G_1 is a p-group with $p = 2$, if G_1 is not the trivial group, then G_1 has a subgroup G_2 of index 2. Let F be the fixed field of G_2. Then F has degree 2 over $\mathbb{R}(i)$. But we saw that every element of $\mathbb{R}(i)$ has a square root, so $\mathbb{R}(i)$ has no extension of degree 2. So G_1 is the trivial group and $K = \mathbb{R}(i)$.

Example 6. Let $f(X)$ be an irreducible polynomial over a field k, and assume that f is seperable. Then the Galois group G of the splitting field is represented as a group of permutations of the n roots, where $n = \deg f$. Whenever one has a criterion for a subgroupn of S_n to be the full symmetric group S_n, then one can see if it applies to the Galois group of f, regarded as a group of permutations of the roots of f. For example, if p is prime, S_p is generated by $[123 \cdots p]$ and any transposition this gives us the following result

Theorem 8. Let $f(X)$ be an irreducible polynomial with rational coefficients and of degree p prime. If f has precisely two nonreal roots in the complex numbers, then the Galois group of f is S_p.

Proof. The order of G is divisible by p, and hence by Sylow's theorem G contains an element of order p. Since G is a subgroup of S_p which has order $p!$, it follows that an element of order p can be represented by a p-cycle $[123 \cdots p]$ after suitable ordereing of the roots, because any smaller cycle has order less than p, so relatively prime to p. But the pair of complex conjugates roots shows that complex conjugation induces a transposition in G. Hence the group is all S_p. □

Index