Normal Function Field Extensions

Unit 19

Gil Cohen

January 3, 2025

Overview

Group actions

Groups allow us to study the symmetries of an object though this connection is sometimes missed in the abstract study of groups. We quickly recap it.

Definition 1

Let X be a set and G a group. A group action α of G on X is a function

$$\alpha : G \times X \to X$$
$$(g, x) \mapsto gx$$

satisfying:

1. $ex = x$; and
2. $g(hx) = (gh)x$,

for all $x \in X$, $g, h \in G$.

The group G is said to act on X.

Group actions

Note that for every fixed $g \in G$, the function

$$\begin{aligned} \varphi_g : X &\to X \\ x &\mapsto gx \end{aligned}$$

is a bijection. Indeed,

$$\begin{aligned} \varphi_g(x) = \varphi_g(y) \quad &\Longrightarrow \quad gx = gy \\ &\Longrightarrow \quad g^{-1}(gx) = g^{-1}(gy) \\ &\Longrightarrow \quad (g^{-1}g)x = (g^{-1}g)y \\ &\Longrightarrow \quad ex = ey \\ &\Longrightarrow \quad x = y. \end{aligned}$$

Moreover,

$$\varphi_g(g^{-1}x) = g(g^{-1}x) = (gg^{-1})(x) = ex = x.$$

Group actions and symmetries

Informally, a symmetry of an object is doing something to it that does not change it.

Formally, A symmetry of a set X is a bijection $\varphi : X \to X$. The set of all symmetries of X, denoted $\mathrm{Sym}(X)$, is a group under composition.

By the previous observation, if G acts on X then every $g \in G$ gives rise to an element $\varphi_g \in \mathrm{Sym}(X)$. Moreover, the map

$$G \to \mathrm{Sym}(X)$$
$$g \mapsto \varphi_g$$

is a group homomorphism since $e \mapsto \mathrm{id}_X$ and

$$\varphi_{gh} = \varphi_g \varphi_h.$$

Indeed, for every $x \in X$,

$$\varphi_{gh}(x) = (gh)x = g(hx) = g\varphi_h(x) = \varphi_g(\varphi_h(x)) = (\varphi_g\varphi_h)(x).$$

From here on we denote φ_g by g.

Transitive actions and orbits

Definition 2

An action of G on $X \neq \emptyset$ is called transitive if

$$\forall x, y \in X \quad \exists g \in G \quad \text{s.t.} \quad gx = y.$$

Definition 3

The orbit of an element $x \in X$ under the action of G is

$$Gx = \{gx \mid g \in G\}.$$

The orbits form a partition of X, hence, they give rise to an equivalence relation:

$$x \sim y \quad \iff \quad Gx = Gy.$$

Note that a group action is transitive iff it has a single orbit.

Definition 4

The set of all orbits of X under the action of G, denoted X/G, is called the quotient of the action.

The stabilizer

When $gx = x$ we say that g fixes x or that x is a fixed point of g.

Definition 5

For $x \in X$ the stabilizer subgroup of G with respect to x is given by

$$G_x = \{g \in G \mid gx = x\}.$$

Observe that for $x, y \in X$ s.t. $y = gx$ the two stabilizers satisfy

$$G_y = gG_xg^{-1}.$$

Thus, the stabilizers of elements in the same orbit are conjugate to each other.

The orbit-stabilizer theorem

Fix $x \in X$. Then,

$$\begin{aligned} gx = hx \quad &\iff \quad h^{-1}gx = x \\ &\iff \quad h^{-1}g \in G_x \\ &\iff \quad gG_x = hG_x. \end{aligned}$$

So

$$|Gx| = |(G : G_x)|.$$

This is despite the fact that G_x may not be normal (so G/G_x is not a group). For finite groups,

$$|x\text{'s orbit}| = |Gx| = \frac{|G|}{|G_x|} = \frac{|G|}{|x\text{'s stabilizer}|}.$$

This result is called the orbit-stabilizer theorem.

Overview

Normal field extensions

Definition 6 (Normal field extensions)

An algebraic extension L/K is said to be normal if every irreducible polynomial $f(x) \in \mathsf{K}[x]$ that has a root $\alpha \in \mathsf{L}$ factors to linear factors in $\mathsf{L}[x]$.

Theorem 7

Let L/K be an algebraic extension and assume $\mathsf{L} \subseteq \bar{\mathsf{K}}$. TFAE

1. L/K *is normal.*
2. L *is the splitting field of some* $\{f_\alpha(x) \in \mathsf{K}[x]\}_\alpha$.
3. *Every automorphism of* $\bar{\mathsf{K}}/\mathsf{K}$ *maps* L *to* L.
4. *For every* $\alpha \in \mathsf{L}$*, all conjugates of* α *over* K *are in* K.

Overview

Separable polynomials

Definition 8 (Separability without referring to an algebraic closure)

Let K be a field. An irreducible polynomial $f(x) \in \mathrm{K}[x]$ is separable if it is has distinct roots in any field extension of K.

Definition 9 (Separability by referring to an algebraic closure)

Let K be a field and $\bar{\mathrm{K}}$ an algebraic closure of K. An irreducible polynomial $f(x) \in \mathrm{K}[x]$ is separable if it is a product of distinct linear factors in $\bar{\mathrm{K}}[x]$.

In characteristic zero all irreducible polynomials are separable. So from here on, we denote the characteristic by $p > 0$.

Separable elements

Definition 10

Let F/E be a field extension. An element $\alpha \in$ F is separable over E if α is algebraic over E and its minimal polynomial is separable over E.

It is known that

$$\alpha, \beta \text{ are separable} \quad \Longrightarrow \quad \alpha+\beta,\ \alpha\beta,\ \alpha^{-1} \text{ are separable.}$$

Thus, the set of elements in F that are separable over E form a field, denoted by E_s.

Separable and purely inseparable extensions

If $\alpha \in \mathrm{F}$ it not separable then $\exists e \geq 1$ s.t. $\alpha^{p^e} \in \mathrm{E}_s$. Further, the minimal polynomial of α over E_s is $(x-\alpha)^{p^e}$.

The extension F/E_s is purely inseparable, namely, every $\alpha \in \mathrm{F} \setminus \mathrm{E}_s$ is not separable over E_s.

Every algebraic field extension F/E can be decomposed as

$$\begin{tikzcd}
F \arrow[d, dash, "\text{purely inseparable}"] \\
E_s \arrow[d, dash, "\text{max sep extension}"] \\
E
\end{tikzcd}$$

We denote $q = [\mathrm{F} : \mathrm{E}]_i = [\mathrm{F} : \mathrm{E}_s]$.

Overview

Galois extensions

Let F/E be an algebraic field extension. Denote by $\Gamma = \mathrm{Aut}(\mathsf{F}/\mathsf{E})$ the set of automorphisms of F that fix each element of E.

Define the field

$$\mathsf{F}^{\Gamma} = \{x \in \mathsf{F} \mid \forall \sigma \in \Gamma \ \ \sigma(x) = x\}.$$

By Galois Theory,

$$\mathsf{F}^{\Gamma} = \mathsf{E} \quad \Longleftrightarrow \quad \mathsf{F}/\mathsf{E} \text{ is normal and separable.}$$

In such case, F/E is called a Galois extension. For such extensions, the group Γ is denoted $\mathrm{Gal}(\mathsf{F}/\mathsf{E})$. It holds that

$$|\mathrm{Gal}(\mathsf{F}/\mathsf{E})| = [\mathsf{F} : \mathsf{E}].$$

Separable and purely inseparable extensions

Assume F/E is normal and consider E_s as before. We have that q is some power of the characteristic, and that $F^q = E_s$.

$$
\begin{tikzcd}
F \arrow[d, dash, "\text{purely inseparable}"] \\
E_s \arrow[d, dash, "\text{max sep extension}"] \\
E
\end{tikzcd}
$$

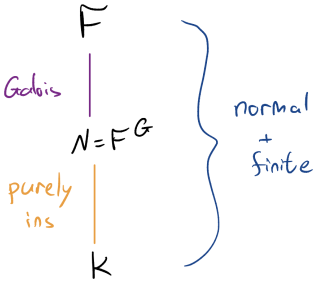
Further, E_s/E is a Galois extension and Aut(F/E) can be identified with the Galois group $G = \mathrm{Gal}(E_s/E)$.

A useful lemma

Lemma 11

Let F/K *be a finite normal extension. Let* $G = \mathrm{Aut}(\mathrm{F}/\mathrm{K})$ *and denote* $\mathrm{N} = \mathrm{F}^G$. *Then,*

1. F/N *is Galois; and*
2. N/K *is purely inseparable.*
3. $\mathrm{Gal}(\mathrm{F}/\mathrm{N}) = G$.



A useful lemma

Proof.

Starting with Item 1, clearly, F/N is normal, and so we focus on separability.

Take $\alpha \in \mathrm{F}$ and let $f(x) \in \mathrm{N}(x)$ be its minimal polynomial over N. Let

$$\alpha = \alpha_1, \alpha_2, \ldots, \alpha_m$$

be the distinct roots of $f(x)$. By normality of F/N these lie in F. Define

$$g(x) = \prod_{i=1}^{m} (x - \alpha_i) \in \mathrm{F}[x].$$

Fix $\sigma \in G$ and $i \in [m]$. Then,

$$0 = \sigma(0) = \sigma(f(\alpha_i)) = f(\sigma(\alpha_i)),$$

where the last equality holds since $\mathrm{N} = \mathrm{F}^G$. Thus, $\sigma(\alpha_i) = \alpha_j$. But σ is one to one and so it acts as a bijection on $\alpha_1, \ldots, \alpha_m$.

A useful lemma

Proof.

Therefore,

$$\forall \sigma \in G \quad \sigma g(x) = \prod_{i=1}^{m} (x - \sigma\alpha_i) = \prod_{i=1}^{m} (x - \alpha_i) = g(x).$$

Hence,

$$g(x) \in \mathrm{F}^G[x] = \mathrm{N}[x].$$

But $f(x)$ is the minimal polynomial of α over N and so $f(x) \mid g(x)$. Clearly, however, $g(x) \mid f(x)$ and so $f(x) = g(x)$ is separable. Thus, α is separable over N.

A useful lemma

Proof.

Moving on to Item 2, we know that

$$[\mathsf{F} : \mathsf{K}]_s = [\mathsf{F} : \mathsf{N}]_s[\mathsf{N} : \mathsf{K}]_s.$$

But by Item 1,

$$[\mathsf{F} : \mathsf{N}]_s = [\mathsf{F} : \mathsf{N}].$$

Galois Theory tells us that

$$[\mathsf{F} : \mathsf{N}] = |\mathrm{Gal}(\mathsf{F}/\mathsf{N})| = |\mathrm{Gal}(\mathsf{F}/\mathsf{F}^G)| = |G| = |\mathrm{Aut}(\mathsf{F}/\mathsf{K})| = [\mathsf{F} : \mathsf{K}]_s.$$

Thus,

$$[\mathsf{F} : \mathsf{N}] = [\mathsf{F} : \mathsf{K}]_s = [\mathsf{F} : \mathsf{N}]_s[\mathsf{N} : \mathsf{K}]_s = [\mathsf{F} : \mathsf{N}][\mathsf{N} : \mathsf{K}]_s.$$

Therefore, $[\mathsf{N} : \mathsf{K}]_s = 1$, namely, N/K is purely inseparable.

Item 3 follows by the above. □

Overview

Isomorphism between function fields

Let F/L, F'/L' be function fields. Let $\sigma : \mathsf{F} \to \mathsf{F}'$ be an isomorphism s.t. $\sigma(\mathsf{L}) = \mathsf{L}'$.

For every valuation υ of F there is a corresponding valuation of F', denoted by $\sigma\upsilon$, that is defined as follows: for $x \in \mathsf{F}'$,

$$(\sigma\upsilon)(x) = \upsilon(\sigma^{-1}(x)).$$

Verify that this is indeed a valuation, and note that

$$\begin{aligned}\mathcal{O}_{\sigma\upsilon} &= \{x \in \mathsf{F}' \mid \sigma\upsilon(x) \geq 0\} \\ &= \{x \in \mathsf{F}' \mid \upsilon(\sigma^{-1}(x)) \geq 0\} \\ &= \{\sigma(y) \mid y \in \mathsf{F} \text{ and } \upsilon(y) \geq 0\} \\ &= \sigma(\mathcal{O}_\upsilon).\end{aligned}$$

Similarly, $\mathfrak{m}_{\sigma\upsilon} = \sigma(\mathfrak{m}_\upsilon)$.

Isomorphism between function fields

By the above, equivalent valuations are mapped by σ to equivalent valuations.

Further, a valuation that is trivial on L is mapped by σ to a valuation that is trivial on L' and vice versa.

Recall that a prime divisor $\mathfrak{p}$ of F/L is an equivalence class of places of F that are trivial on L. Thus, by the above, σ induces a bijection

$$\mathfrak{p} \mapsto \sigma\mathfrak{p}$$

between the prime divisors of F/L and the prime divisors of F'/L'.

Isomorphism between function fields

As the diagram below depicts, σ also induces an isomorphism $\bar{\sigma}$ between the residue fields

$$\bar{\sigma} : \mathsf{F}_{\mathfrak{p}} = \mathcal{O}_{\mathfrak{p}} \big/ \mathfrak{m}_{\mathfrak{p}} \to \mathsf{F}_{\sigma\mathfrak{p}} = \mathcal{O}_{\sigma\mathfrak{p}} \big/ \mathfrak{m}_{\sigma\mathfrak{p}}$$

that is given by $\bar{\sigma}\bar{x} = \overline{\sigma x}$ or, more informatively, $\bar{\sigma}(x + \mathfrak{m}_{\mathfrak{p}}) = \sigma x + \mathfrak{m}_{\sigma\mathfrak{p}}$.

$$\begin{tikzcd}
\mathcal{O}_{\mathfrak{p}} \arrow[r, "\sigma"] \arrow[d] & \mathcal{O}_{\sigma\mathfrak{p}} \arrow[d] \\
\mathcal{O}_{\mathfrak{p}}/\mathfrak{m}_{\mathfrak{p}} = \mathsf{F}_{\mathfrak{p}} \arrow[r, "\bar{\sigma}"] & \mathsf{F}_{\sigma\mathfrak{p}} = \mathcal{O}_{\sigma\mathfrak{p}}/\mathfrak{m}_{\sigma\mathfrak{p}}
\end{tikzcd}$$

In particular, $\deg(\sigma\mathfrak{p}) = \deg(\mathfrak{p})$.

Overview

Normal extensions of function fields

Definition 12

A function field extension F/L over E/K is called normal if F/E is a normal field extension.

Claim 13

If F/L is a normal extension of E/K then L/K is normal.

To prove Claim 13 we first prove

Claim 14

Let E/K be a field extension s.t. K is algebraically closed in E. Then,

$$f \in K[x] \text{ is irreducible} \quad \Longrightarrow \quad f \text{ is irreducible in } E[x].$$

Normal extensions of function fields

Proof.

Let $g(x) \in \mathrm{E}[x]$ be an irreducible factor of $f(x)$ in $\mathrm{E}[x]$. We will prove that $g(x) \in \mathrm{K}[x]$.

In $\bar{\mathrm{E}}[x]$ we can write

$$g(x) = \prod_{i=1}^{m} (x - a_i).$$

But the a_i-s are some of the roots of $f(x)$, and so $a_i \in \bar{\mathrm{K}}$.

The coefficients of $g(x)$ are polynomials in the a_i-s, and so

$$g(x) \in \bar{\mathrm{K}}[x].$$

But $g(x) \in \mathrm{E}[x]$, and so

$$g(x) \in (\bar{\mathrm{K}} \cap \mathrm{E})[x] = \mathrm{K}[x].$$

$\square$

Proof of Claim 13.

We already proved that

$$\mathsf{F}/\mathsf{E} \text{ is algebraic} \quad \Longrightarrow \quad \mathsf{L}/\mathsf{K} \text{ is algebraic.}$$

Take $f(x) \in \mathsf{K}[x]$ irreducible with a root $\alpha \in \mathsf{L}$. We need to prove that $f(x)$ splits in $\mathsf{L}[x]$.

By Claim 14, $f(x)$ is irreducible over E. Further, $\alpha \in \mathsf{L} \subseteq \mathsf{F}$, and so as F/E is normal, $f(x)$ splits over F.

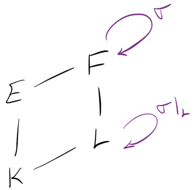
Now, $f(x) \in \mathsf{K}[x] \subseteq \mathsf{L}[x]$ and so all roots of $f(x)$ in F are algebraic over L, and so they belong to L. $\square$

$$\begin{tikzcd}
 & F \arrow[d, dash] \\
E \arrow[ur, dash] \arrow[d, dash] & L \\
K \arrow[ur, dash] &
\end{tikzcd}$$

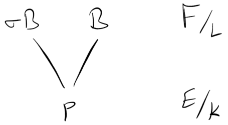
Normal extensions of function fields

Assume again that F/L is a normal extension of E/K.

Consider $\sigma \in \mathrm{Aut}(\mathsf{F}/\mathsf{E})$. In particular, $\sigma|_K = \mathrm{id}_\mathsf{K}$. As L/K is normal, we have that $\sigma(\mathsf{L}) = \mathsf{L}$. Namely, $\sigma|_\mathsf{L} \in \mathrm{Aut}(\mathsf{L}/\mathsf{K})$.



As $\sigma|_\mathsf{E} = \mathrm{id}_\mathsf{E}$ we have that for a prime divisor $\mathfrak{P}$ of F/L lying over a prime divisor $\mathfrak{p}$ of E/K it holds that $\sigma\mathfrak{P}$ is also a prime divisor of F/L that lies over $\sigma\mathfrak{p} = \mathfrak{p}$.



Normal extensions of function fields

$$
\begin{tikzcd}
L \arrow[r, dash] \arrow[d, dash] & F_{\mathfrak{P}} \arrow[d, dash] \\
K \arrow[r, dash] & E_{\mathfrak{p}}
\end{tikzcd}
$$

We have that

$$
\begin{aligned}
f(\sigma\mathfrak{P}/\mathfrak{p}) &= [\mathsf{L} : \mathsf{K}] \cdot \frac{\deg \sigma\mathfrak{P}}{\deg \mathfrak{p}} = [\mathsf{L} : \mathsf{K}] \cdot \frac{\deg \mathfrak{P}}{\deg \mathfrak{p}} = f(\mathfrak{P}/\mathfrak{p}), \\
e(\sigma\mathfrak{P}/\mathfrak{p}) &= (\upsilon_{\sigma\mathfrak{P}}(\mathsf{F}^{\times}) : \upsilon_{\sigma\mathfrak{p}}(\mathsf{E}^{\times})) = (\upsilon_{\mathfrak{P}}(\mathsf{F}^{\times}) : \upsilon_{\mathfrak{p}}(\mathsf{E}^{\times})) = e(\mathfrak{P}/\mathfrak{p}).
\end{aligned}
$$

Thus, for every prime divisor $\mathfrak{p}$ of E/K, $\mathrm{Aut}(\mathsf{F}/\mathsf{E})$ acts on the prime divisors lying over $\mathfrak{p}$, keeping the residual degree and ramification index intact.

We turn to prove that this action is transitive.

Normal extensions of function fields

From hereon, let F/L be a normal finite extension of E/K. We let E_s be the maximal separable extension of E in F and denote

$$q = [\mathrm{F} : \mathrm{E}]_i = [\mathrm{F} : \mathrm{E}_s].$$

From Galois Theory, we know that q is some power of the characteristic p, and that $\mathrm{F}^q = \mathrm{E}_s$.

Further, E_s/E is a Galois extension and $\mathrm{Aut}(\mathrm{F}/\mathrm{E})$ can be identified with the Galois group $G = \mathrm{Gal}(\mathrm{E}_s/\mathrm{E})$.

$$\begin{tikzcd} F \arrow[d, dash, "\text{purely inseparable}"] \\ E_s \arrow[d, dash, "\text{max sep extension}"] \\ E \end{tikzcd}$$

Normal extensions of function fields

If $z \in \mathsf{E}_s$ then

$$\prod_{\sigma \in G} \sigma z$$

is fixed by all elements of $G = \mathrm{Gal}(\mathsf{E}_s/\mathsf{E})$ since for every $\tau \in G$,

$$\tau \prod_{\sigma \in G} \sigma z = \prod_{\sigma \in G} \tau\sigma z = \prod_{\sigma \in G} \sigma z.$$

Thus, $\prod_{\sigma \in G} \sigma z \in \mathsf{E}_s^G = \mathsf{E}$.

For every $x \in \mathsf{F}$ we have that $x^q \in \mathsf{E}_s$, and so

$$\prod_{\sigma \in G} \sigma(x^q) \in \mathsf{E}.$$

This way one can define the norm of finite normal extensions:

$$\mathrm{N}_{\mathsf{F}/\mathsf{E}}(x) \triangleq \left(\prod_{\sigma \in G} \sigma x\right)^q \in \mathsf{E}.$$

Normal extensions of function fields

Theorem 15

Let F/L *be a finite normal function field extension of* E/K*. Let* $\mathfrak{p}$ *be a prime divisor of* E/K*. Then,* Aut(F/E) *acts transitively on the set of prime divisors lying over* $\mathfrak{p}$*.*

That is, for every two prime divisors $\mathfrak{P}, \mathfrak{P}'$ *of* F/L *that lie over* $\mathfrak{p}$*,*

$$\exists \sigma \in \mathrm{Aut}(\mathrm{F}/\mathrm{E}) \quad s.t. \quad \sigma\mathfrak{P} = \mathfrak{P}'.$$

Proof.

Assume that $\mathfrak{P}' \neq \sigma\mathfrak{P}$ for all $\sigma \in G = \mathrm{Aut}(\mathrm{F}/\mathrm{E})$. Then, the corresponding orbits are disjoint

$$\{\sigma\mathfrak{P}' \mid \sigma \in G\} \cap \{\sigma\mathfrak{P} \mid \sigma \in G\} = \emptyset.$$

By the WAT $\exists x \in \mathrm{F}$ s.t.

$$\forall \sigma \in G \quad v_{\sigma\mathfrak{P}}(x) > 0 \;\text{ and }\; v_{\sigma\mathfrak{P}'}(x) < 0.$$

Normal extensions of function fields

Proof.

Recall that $q = [\mathsf{F} : \mathsf{E}_s]$, $G = \mathrm{Gal}(\mathsf{E}_s/\mathsf{E})$, and consider

$$y = \mathrm{N}_{\mathsf{F}/\mathsf{E}}(x) = \left(\prod_{\sigma \in G} \sigma x \right)^q \in \mathsf{E}.$$

Then,

$$\upsilon_{\mathfrak{P}}(y) = q \sum_{\sigma \in G} \upsilon_{\mathfrak{P}}(\sigma x) = q \sum_{\sigma \in G} \upsilon_{\sigma^{-1}\mathfrak{P}}(x) = q \sum_{\sigma \in G} \upsilon_{\sigma\mathfrak{P}}(x) > 0.$$

As $y \in \mathsf{E}$, we can also consider

$$\upsilon_{\mathfrak{p}}(y) = \frac{1}{e(\mathfrak{P}/\mathfrak{p})} \upsilon_{\mathfrak{P}}(y) > 0.$$

However, by considering $\upsilon_{\mathfrak{P}'}$ instead of $\mathfrak{P}$ we will reach the opposite conclusion, $\upsilon_{\mathfrak{p}}(y) < 0$, and the proof follows. □

Overview

The decomposition group

Again let $G = \mathrm{Aut(F/E)}$, $\mathfrak{p}$ as above and $\mathfrak{P}$ a prime divisor lying over $\mathfrak{p}$.

The stabilizer of $\mathfrak{P}$ is called the decomposition group

$$D(\mathfrak{P}) = \{\sigma \in G \mid \sigma\mathfrak{P} = \mathfrak{P}\}.$$

Since G acts transitively on the prime divisors lying over $\mathfrak{p}$,

$$r \triangleq |G\mathfrak{P}| = \text{number of prime divisors of F/L lying over } \mathfrak{p}.$$

Thus, by the orbit-stabilizer theorem,

$$r = (G : D(\mathfrak{P})). \tag{1}$$

Residue fields in normal extensions

Theorem 16

Let F/L *be an extension of* E/K*, and consider prime divisors* $\mathfrak{P}/\mathfrak{p}$*. Assume* F/E *is normal and finite. Then, the extension of the residue fields* $\mathsf{F}_{\mathfrak{P}}/\mathsf{E}_{\mathfrak{p}}$ *is normal and finite.*

We already saw that $\mathsf{F}_{\mathfrak{P}}/\mathsf{E}_{\mathfrak{p}}$ is finite since F/E is. In particular, $\mathsf{F}_{\mathfrak{P}}/\mathsf{E}_{\mathfrak{p}}$ is algebraic. We turn to prove normality. To this end, we start by proving the following claim.

Claim 17

For every $z \in \mathsf{F}_{\mathfrak{P}} = \mathcal{O}_{\mathfrak{P}}/\mathfrak{m}_{\mathfrak{P}}$ there is a representative $y \in \mathcal{O}_{\mathfrak{P}}$ s.t.

1. $\upsilon_{\mathfrak{P}}(\sigma y) \geq 0$ for all $\sigma \in G$; and
2. $\upsilon_{\mathfrak{P}}(\sigma y) > 0$ for all $\sigma \in G \setminus D(\mathfrak{P})$.

Residue fields in normal extensions

Proof. (of Claim 17)

Take any representative $y' \in \mathcal{O}_{\mathfrak{P}}$ for z, namely, $z = y' + \mathfrak{m}_{\mathfrak{P}}$. Note that for $\sigma \in G \setminus D(\mathfrak{P})$, we have $\mathfrak{P} \neq \sigma^{-1}\mathfrak{P}$. By the WAT, $\exists y \in$ F s.t.

1. $\upsilon_{\mathfrak{P}}(y - y') > 0$; and
2. $\upsilon_{\sigma^{-1}\mathfrak{P}}(y) > 0 \quad \forall \sigma \in G \setminus D(\mathfrak{P})$.

As $\upsilon_{\mathfrak{P}}(y') \geq 0$ and $\upsilon_{\mathfrak{P}}(y - y') > 0$ we have that $\upsilon_{\mathfrak{P}}(y) \geq 0$, namely, $y \in \mathcal{O}_{\mathfrak{P}}$.

Item (2) above implies Item (2) of the claim since $\upsilon_{\mathfrak{P}}(\sigma y) = \upsilon_{\sigma^{-1}\mathfrak{P}}(y)$.

As for Item (1), for $\sigma \in D(\mathfrak{P})$,

$$\upsilon_{\mathfrak{P}}(\sigma y) = \upsilon_{\sigma^{-1}\mathfrak{P}}(y) = \upsilon_{\mathfrak{P}}(y) \geq 0.$$

To conclude the proof, by Item (1),

$$y + \mathfrak{m}_{\mathfrak{P}} = y' + \mathfrak{m}_{\mathfrak{P}} = z.$$

Residue fields in normal extensions

Proof. (of Theorem 16)

Going back to the proof of Theorem 16, we take $z \in \mathsf{F}_{\mathfrak{P}}$ and show that all of its $\mathsf{E}_{\mathfrak{p}}$-conjugates are in $\mathsf{F}_{\mathfrak{P}}$.

With $y = y(z)$ as in Claim 17, consider the polynomial

$$f(X) = \prod_{\sigma \in G} (X - \sigma y)^q = \prod_{\sigma \in G} (X^q - \sigma(y^q)) \in \mathsf{F}[X].$$

Since $\sigma y \in \mathcal{O}_{\mathfrak{P}}$ for all $\sigma \in G$,

$$f(X) \in \mathcal{O}_{\mathfrak{P}}[X].$$

Looking at the right expression, and since $y^q \in \mathsf{E}_s$, we have that $f(X) \in \mathsf{E}_s[X]$.

Observe that the coefficients of $f(X)$ are fixed by G and so, in fact, $f(X) \in \mathsf{E}_s^G[X] = \mathsf{E}[X]$. Thus,

$$f(X) \in (\mathsf{E} \cap \mathcal{O}_{\mathfrak{P}})[X] = \mathcal{O}_{\mathfrak{p}}[X].$$

Residue fields in normal extensions

Proof.

So far,

$$f(X) = \prod_{\sigma \in G} (X - \sigma y)^q \in \mathcal{O}_{\mathfrak{p}}[X].$$

Recall that for $\sigma \in G \setminus D(\mathfrak{P})$ we have $v_{\mathfrak{P}}(\sigma y) > 0$, namely,

$$\sigma y + \mathfrak{m}_{\mathfrak{P}} = \overline{\sigma y} = 0 \quad (\text{in } \mathsf{F}_{\mathfrak{P}} = \mathcal{O}_{\mathfrak{P}}/\mathfrak{m}_{\mathfrak{P}}).$$

Thus, the reduction of $f(X) \in \mathcal{O}_{\mathfrak{P}}[X]$ to $\bar{f}(X) \in \mathsf{F}_{\mathfrak{P}}[X]$ is

$$\begin{aligned}\bar{f}(X) &= \prod_{\sigma \in G} (X - \overline{\sigma y})^q \\ &= X^{q|G \setminus D(\mathfrak{P})|} \prod_{\sigma \in D(\mathfrak{P})} (X - \overline{\sigma y})^q \in \mathsf{E}_{\mathfrak{p}}[X].\end{aligned}$$

Residue fields in normal extensions

Proof.

We conclude that the polynomial

$$g(X) = \prod_{\sigma \in D(\mathfrak{P})} (X - \overline{\sigma y})^q \in \mathsf{E}_{\mathfrak{p}}[X]$$

has all its roots in $\mathsf{F}_{\mathfrak{P}}$ as indeed $\sigma y \in \mathcal{O}_{\mathfrak{P}}$.

Now, taking $\sigma = \mathrm{id} \in D(\mathfrak{P})$, we see that

$$g(z) = g(\bar{y}) = 0.$$

Thus, the minimal polynomial of z over $\mathsf{E}_{\mathfrak{p}}$ divides $g(X)$.

We conclude that all $\mathsf{E}_{\mathfrak{p}}$-conjugates of z are in $\mathsf{F}_{\mathfrak{P}}$, and so $\mathsf{F}_{\mathfrak{P}}/\mathsf{E}_{\mathfrak{p}}$ is normal. □

Residue fields in normal extensions

Recall

$$D(\mathfrak{P}) = \{\sigma \in \mathrm{Aut}(\mathsf{F}/\mathsf{E}) \mid \sigma\mathfrak{P} = \mathfrak{P}\}.$$

Consider the map

$$\begin{aligned} \psi : D(\mathfrak{P}) &\to \mathrm{Aut}(\mathsf{F}_{\mathfrak{P}}/\mathsf{E}_{\mathfrak{p}}) \\ \sigma &\mapsto \bar{\sigma} \end{aligned}$$

where $\bar{\sigma}\bar{x} = \overline{\sigma x}$ for all $x \in \mathcal{O}_{\mathfrak{P}}$ (namely, $\bar{\sigma}(x + \mathfrak{m}_{\mathfrak{P}}) = \sigma x + \mathfrak{m}_{\mathfrak{P}}$). As $\sigma \in D(\mathfrak{P})$ we have that

$$x \in \mathcal{O}_{\mathfrak{P}} \quad \Longrightarrow \quad \sigma x \in \mathcal{O}_{\sigma\mathfrak{P}} = \mathcal{O}_{\mathfrak{P}}.$$

$\bar{\sigma}$ acts as the identity on $\mathsf{E}_{\mathfrak{p}}$. Indeed, take $x \in \mathsf{E}$, then

$$\bar{\sigma}(x + \mathfrak{m}_{\mathfrak{P}}) = \sigma x + \mathfrak{m}_{\mathfrak{P}} = x + \mathfrak{m}_{\mathfrak{P}}.$$

It is easy to check that $\bar{\sigma}$ is indeed an automorphism.

Residue fields in normal extensions

Theorem 18

ψ is an epiomorphism

Proof.

We first show that ψ is a group homomorphism. Take $\sigma, \tau \in D(\mathfrak{P})$. We wish to prove that $\psi(\sigma\tau) = \psi(\sigma)\psi(\tau)$. To this end, take $x \in \mathcal{O}_{\mathfrak{P}}$.

We have that

$$\begin{aligned}\psi(\sigma)\psi(\tau)(x + \mathfrak{m}_{\mathfrak{P}}) &= \psi(\sigma)(\tau x + \mathfrak{m}_{\mathfrak{P}}) \\ &= \sigma(\tau x) + \mathfrak{m}_{\mathfrak{P}} \\ &= (\sigma\tau)x + \mathfrak{m}_{\mathfrak{P}} \\ &= \psi(\sigma\tau)(x + \mathfrak{m}_{\mathfrak{P}}).\end{aligned}$$

Residue fields in normal extensions

Proof.

We turn to show that ψ is onto.

Let N be the fixed field of $\mathrm{Aut}(F_{\mathfrak{P}}/E_{\mathfrak{p}})$. By Lemma 11, we know that $N/E_{\mathfrak{p}}$ is purely inseparable and that $F_{\mathfrak{P}}/N$ is Galois.

$$\begin{tikzcd}
F_{\mathfrak{P}} \arrow[d, dash, "\text{Galois}"'] & \\
N \arrow[d, dash, "\text{purely inseparable}"'] & \text{fixed field of } \mathrm{Aut}(F_{\mathfrak{P}}/E_{\mathfrak{p}}) \\
E_{\mathfrak{p}} &
\end{tikzcd}$$

Residue fields in normal extensions

Proof.

As $\mathrm{F}_{\mathfrak{P}}/\mathrm{N}$ is Galois and finite, by the primitive element theorem,

$$\exists z \in \mathrm{F}_{\mathfrak{P}} \quad \text{s.t.} \quad \mathrm{F}_{\mathfrak{P}} = \mathrm{N}(z).$$

As in the proof of Theorem 16, we can find $y \in \mathcal{O}_{\mathfrak{P}}$ s.t. $\bar{y} = z$ and that

$$g(X) = \prod_{\sigma \in D(\mathfrak{P})} (X - \overline{\sigma y})^q \in \mathrm{E}_{\mathfrak{p}}[X].$$

Recall that $g(z) = 0$.

Take $\tau \in \mathrm{Aut}(\mathrm{F}_{\mathfrak{P}}/\mathrm{E}_{\mathfrak{p}})$ and note that τz is also a root of g. Indeed,

$$0 = \tau(0) = \tau(g(z)) = g(\tau(z)).$$

Hence, $\exists \sigma \in D(\mathfrak{P})$ s.t.

$$\tau z = \overline{\sigma y} = \bar{\sigma}\bar{y} = \bar{\sigma} z.$$

Residue fields in normal extensions

Proof.

So far we wrote

$$\mathsf{F}_{\mathfrak{P}} = \mathsf{N}(z)$$

for some $z \in \mathsf{F}_{\mathfrak{P}}$, and proved that

$$\forall \tau \in \mathrm{Aut}(\mathsf{F}_{\mathfrak{P}}/\mathsf{E}_{\mathfrak{p}}) \quad \exists \sigma \in D(\mathfrak{P}) \quad \text{s.t.} \quad \tau z = \bar{\sigma} z.$$

As $\bar{\sigma}, \tau \in \mathrm{Aut}(\mathsf{F}_{\mathfrak{P}}/\mathsf{E}_{\mathfrak{p}})$,

$$\bar{\sigma}|_{\mathsf{N}} = \tau|_{\mathsf{N}} = \mathrm{id}_{\mathsf{N}}.$$

We conclude that $\bar{\sigma} = \tau$. Namely, $\tau = \psi(\sigma)$ for some $\sigma \in \mathcal{D}(\mathfrak{P})$, and so ψ is onto. $\square$

Overview

The inertia group

So far we saw the group epimorphism

$$\psi : D(\mathfrak{P}) \to \mathrm{Aut}(\mathsf{F}_{\mathfrak{P}}/\mathsf{E}_{\mathfrak{p}}).$$

Definition 19

The kernel of ψ, denoted by $\mathrm{I}(\mathfrak{P}/\mathfrak{p})$ (or sometimes $\mathrm{I}(\mathfrak{P})$ for short) is called the inertia group of $\mathfrak{P}$.

Since ψ is an epimorphism, we have that

$$|D(\mathfrak{P})| = |\mathrm{I}(\mathfrak{P})| \cdot |\mathrm{Aut}(\mathsf{F}_{\mathfrak{P}}/\mathsf{E}_{\mathfrak{p}})|. \tag{2}$$

Overview

Some equalities

Corollary 20

Assume F/E *is finite and normal. Denote* $e = e(\mathfrak{P}/\mathfrak{p})$, $f = f(\mathfrak{P}/\mathfrak{p})$. *Then,*

1. $\forall \sigma \in G \quad e(\sigma\mathfrak{P}) = e$ *and* $f(\sigma\mathfrak{P}) = f$.
2. $[\mathsf{F} : \mathsf{E}] = efr$ *where* r *is the number of prime divisors of* F *lying over* $\mathfrak{p}$.
3. $e = \frac{[\mathsf{F}:\mathsf{E}]_i}{[\mathsf{F}_{\mathfrak{P}}:\mathsf{E}_{\mathfrak{p}}]_i} \cdot |\mathrm{I}(\mathfrak{P}/\mathfrak{p})|$.
4. $ef = [\mathsf{F} : \mathsf{E}]_i \cdot |D(\mathfrak{P}/\mathfrak{p})|$.

Proof.

Item 1 follows immediately by the discussion so far, and since $\sigma\mathfrak{p} = \mathfrak{p}$.

Item 2 follows by Item 1 and by the fundamental equality.

Some equalities

Proof.

We turn to prove Item 3, namely,

$$e = \frac{[\mathsf{F} : \mathsf{E}]_i}{[\mathsf{F}_{\mathfrak{P}} : \mathsf{E}_{\mathfrak{p}}]_i} \cdot |\mathrm{I}(\mathfrak{P}/\mathfrak{p})|.$$

By Item 2, $e = \frac{[\mathsf{F}:\mathsf{E}]}{fr}$. Consider then

$$[\mathsf{F} : \mathsf{E}] = [\mathsf{F} : \mathsf{E}_s][\mathsf{E}_s : \mathsf{E}] = [\mathsf{F} : \mathsf{E}]_i \cdot |G|$$
$$f = [\mathsf{F}_{\mathfrak{P}} : \mathsf{E}_{\mathfrak{p}}] = [\mathsf{F}_{\mathfrak{P}} : \mathsf{E}_{\mathfrak{p}}]_i \cdot a,$$

where $a = [\mathsf{F}_{\mathfrak{P}} : \mathsf{E}_{\mathfrak{p}}]_s = |\mathrm{Aut}(\mathsf{F}_{\mathfrak{P}}/\mathsf{E}_{\mathfrak{p}})|$.

Using the orbit-stabilizer theorem we proved that $r = (G : D(\mathfrak{P}))$, and so

$$|G| = r|D(\mathfrak{P})| = r|\mathrm{I}(\mathfrak{P})| \cdot a,$$

where we used Equation 2.

Some equalities

Proof.

So far,

$$\begin{aligned} [\mathsf{F} : \mathsf{E}] &= [\mathsf{F} : \mathsf{E}]_i \cdot |G|. \\ f &= [\mathsf{F}_{\mathfrak{P}} : \mathsf{E}_{\mathfrak{p}}]_i \cdot a. \\ |G| &= r|D(\mathfrak{P})| = r|\mathrm{I}(\mathfrak{P})| \cdot a. \end{aligned}$$

Thus,

$$e = \frac{[\mathsf{F} : \mathsf{E}]}{fr} = \frac{[\mathsf{F} : \mathsf{E}]_i}{[\mathsf{F}_{\mathfrak{P}} : \mathsf{E}_{\mathfrak{p}}]_i} \cdot \frac{|G|}{ar} = \frac{[\mathsf{F} : \mathsf{E}]_i}{[\mathsf{F}_{\mathfrak{P}} : \mathsf{E}_{\mathfrak{p}}]_i} \cdot |\mathrm{I}(\mathfrak{P})|.$$

This proves Item 3.

Some equalities

Proof.

Recall that

$$[\mathsf{F} : \mathsf{E}] = [\mathsf{F} : \mathsf{E}]_i \cdot |G|.$$
$$|G| = r|D(\mathfrak{P})|.$$

We turn to prove Item 4, namely,

$$ef = [\mathsf{F} : \mathsf{E}]_i \cdot |D(\mathfrak{P}/\mathfrak{p})|.$$

We have that

$$ef = \frac{[\mathsf{F} : \mathsf{E}]}{r} = \frac{[\mathsf{F} : \mathsf{E}]_i \cdot |G|}{r} = \frac{[\mathsf{F} : \mathsf{E}]_i \cdot r|\mathcal{D}(\mathfrak{P})|}{r} = [\mathsf{F} : \mathsf{E}]_i \cdot |D(\mathfrak{P})|,$$

which completes the proof. $\square$

Some equalities

Corollary 21

Assume F/E *is a finite Galois extension and that* K *is a perfect field.*

Denote $e = e(\mathfrak{P}/\mathfrak{p})$, $f = f(\mathfrak{P}/\mathfrak{p})$ *and* $G = \mathrm{Gal}(\mathrm{F}/\mathrm{E})$*. Then,*

1. $\forall \sigma \in G \quad e(\sigma\mathfrak{P}) = e$ *and* $f(\sigma\mathfrak{P}) = f$.
2. $[\mathrm{F} : \mathrm{E}] = efr$ *where* r *is the number of prime divisors of* F *lying over* $\mathfrak{p}$.
3. $e = |\mathrm{I}(\mathfrak{P}/\mathfrak{p})|$.
4. $ef = |D(\mathfrak{P}/\mathfrak{p})|$.