26.02.2024
Algebraheft ①
A. Ram

Proof Machine

Proof type 0: To show: A

To show: replace A with the definition of A

Proof type I: To show: LHS = RHS

LHS = ... = stuff

RHS = . . . = stuff

Proof type II: To show: If A then B

Assume A

To show: B.

Proof type III To show: There exists C such that (a) ___
(b) ___

Let C = ______

To show: (a) ______
(b) ______

26.02.2024
Algebra Lect 1
A. Ram

Definitions: Fields

A **field** is a set with two functions...

Examples: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, ...

Let $\mathbb{F}$ be a field. A **subfield of $\mathbb{F}$** is a subset $\mathbb{E} \subseteq \mathbb{F}$ such that

(a) $0 \in \mathbb{F}$

(b) $1 \in \mathbb{F}$

(c) If $e_1, e_2 \in \mathbb{F}$ then $e_1 + e_2 \in \mathbb{F}$

(d) If $e_1, e_2 \in \mathbb{F}$ then $e_1 e_2 \in \mathbb{F}$

(e) If $e \in \mathbb{F}$ and $e \neq 0$ then $e^{-1} \in \mathbb{F}$.

(f) If $e \in \mathbb{F}$ then $-e \in \mathbb{F}$

Let $\mathbb{F}$ be a field. An **automorphism of $\mathbb{F}$** is a function $\sigma : \mathbb{F} \to \mathbb{F}$ such that

(a) if $a_1, a_2 \in \mathbb{F}$ then $\sigma(a_1 + a_2) = \sigma(a_1) + \sigma(a_2)$

(b) if $a_1, a_2 \in \mathbb{F}$ then $\sigma(a_1 a_2) = \sigma(a_1)\sigma(a_2)$

(c) σ is a bijection.

The **automorphism group of $\mathbb{F}$** is

$$\mathrm{Aut}(\mathbb{F}) = \{\sigma : \mathbb{F} \to \mathbb{F} \mid \sigma \text{ is an automorphism}\}$$

with operation composition of functions.

Definitions: Galois operations

Let $\mathbb{F}$ be a field.

Let $\mathbb{E}$ be a subfield of $\mathbb{F}$.

$$Aut_{\mathbb{E}}(\mathbb{F}) = \left\{ \sigma \in Aut(\mathbb{F}) \,\middle|\, \begin{array}{l} \text{if } e \in \mathbb{E} \text{ then} \\ \sigma(e) = e \end{array} \right\}$$

Let H be a subgroup of $Aut(\mathbb{F})$.

$$\mathbb{F}^H = \{ e \in \mathbb{F} \mid \text{if } \sigma \in H \text{ then } \sigma(e) = e \}.$$

Remark: $\mathbb{F}$ is an $\mathbb{E}$-vector space

$\dim_{\mathbb{E}}(\mathbb{F})$ is the number of elements in a basis of $\mathbb{F}$ as an $\mathbb{E}$-vector space

Common notation: $[\mathbb{E} : \mathbb{F}] = \dim_{\mathbb{E}}(\mathbb{F})$.

Proposition Let $\mathbb{F}$ be a field.

Let H be a subgroup of $Aut(\mathbb{F})$

Then $\mathbb{F}^H$ is a subfield of $\mathbb{F}$.

<u>Proof</u> To show: $\mathbb{F}^H$ is a subfield of $\mathbb{F}$.

To show: (a) $0 \in \mathbb{F}^H$

(b) $1 \in \mathbb{F}^H$

(c) If $e_1, e_2 \in \mathbb{F}^H$ then $e_1 + e_2 \in \mathbb{F}^H$

(d) If $e_1, e_2 \in \mathbb{F}^H$ then $e_1 e_2 \in \mathbb{F}^H$

(e) If $e \in \mathbb{F}^H$ and $e \neq 0$ then $e^{-1} \in \mathbb{F}^H$.

(f) If $e \in \mathbb{F}^H$ then $-e \in \mathbb{F}^H$

(d) Assume $e_1, e_2 \in \mathbb{F}^H$

To show: $e_1 e_2 \in \mathbb{F}^H$

To show: If $\sigma \in H$ then $\sigma(e_1 e_2) = e_1 e_2$.

Assume $\sigma \in H$

Since $e_1, e_2 \in \mathbb{F}^H$ then $\sigma(e_1) = e_1$ and $\sigma(e_2) = e_2$

To show: $\sigma(e_1 e_2) = e_1 e_2$.

$\sigma(e_1 e_2) = \sigma(e_1)\sigma(e_2) = e_1 e_2$.

(e) Assume $e \in \mathbb{F}^H$ and $e \neq 0$.

To show: $e^{-1} \in \mathbb{F}^H$.

To show: If $\sigma \in H$ then $\sigma(e^{-1}) = e^{-1}$.

Assume $\sigma \in H$

To show: $\sigma(e^{-1}) = e^{-1}$.

To show: $\sigma(e^{-1}) e = 1$.

Since $e \in \mathbb{F}^H$ then $\sigma(e) = e$.

So
$$\sigma(e^{-1})e = \sigma(e^{-1})\sigma(e) = \sigma(e^{-1}e) = \sigma(1)$$
$$= 1, \text{ by part (b)}.$$

So $$\sigma(e^{-1}) = \sigma(e^{-1})\cdot 1 = \sigma(e^{-1})e\cdot e^{-1} = 1\cdot e^{-1} = e^{-1}.$$

(c) Assume $e_1, e_2 \in \mathbb{F}^H$

To show: $e_1 + e_2 \in \mathbb{F}^H$

To show: If $\sigma \in H$ then $\sigma(e_1 + e_2) = e_1 + e_2$.

Assume $\sigma \in H$.

To show: $\sigma(e_1 + e_2) = e_1 + e_2$.

Since $\sigma \in H$ then $\sigma(e_1) = e_1$ and $\sigma(e_2) = e_2$.

Then
$$\sigma(e_1 + e_2) = \sigma(e_1) + \sigma(e_2) = e_1 + e_2.$$

So $e_1 + e_2 \in \mathbb{F}^H$.

(b) To show: $1 \in \mathbb{F}^H$

To show: If $\sigma \in H$ then $\sigma(1) = 1$.

Assume $\sigma \in H$.

To show: $\sigma(1) = 1$.

To show: If $y \in \mathbb{F}$ then $\sigma(1)y = y$.

Assume $y \in \mathbb{F}$

26.04.2024 6

Algebra
Lect. 1.
A. Ram

Since σ is surjective there exists $x \in \mathbb{F}$ such that $\sigma(x) = y$.

Then
$$\sigma(1)y = \sigma(1)\sigma(x) = \sigma(1\cdot x) = \sigma(x) = y.$$

So $\sigma(1) = \sigma(1)\cdot 1 = 1$.

(a) To show: $0 \in \mathbb{F}^H$.

To show: If $\sigma \in H$ then $\sigma(0) = 0$.

Assume $\sigma \in H$

To show: $\sigma(0) = 0$.

$$\sigma(0) = \sigma(0+0) = \sigma(0) + \sigma(0).$$

Add $-\sigma(0)$ to each side to get
$$\sigma(0) - \sigma(0) = \sigma(0) + \sigma(0) - \sigma(0).$$

So $0 = \sigma(0) + 0 = \sigma(0)$.

So $0 \in \mathbb{F}^H$.

//.