Galois Theory notes

arnaucube

2023-2024

Abstract

Notes taken while studying Galois Theory, mostyly from Ian Stewart's book "Galois Theory" [1].

Usually while reading books and papers I take handwritten notes in a notebook, this document contains some of them re-written to $LaTeX$.

The notes are not complete, don't include all the steps neither all the proofs.

Contents

1 Recap on the degree of field extensions

Definition 4.10. A *simple extension* is $L : K$ such that $L = K(\alpha)$ for some $\alpha \in L$.

Example 4.11. Beware, $L = \mathbb{Q}(i, -i, \sqrt{5}, -\sqrt{5}) = \mathbb{Q}(i, \sqrt{5}) = \mathbb{Q}(i + \sqrt{5})$.

Definition 5.5. Let $L : K$, suppose $\alpha \in L$ is algebraic over K. Then, the *minimal polynomial* of α over K is the unique monic polynomial m over K, $m(t) \in K[t]$, of smallest degree such that $m(\alpha) = 0$.
eg.: $i \in \mathbb{C}$ is algebraic over $\mathbb{R}$. The minimal polynomial of i over $\mathbb{R}$ is $m(t) = t^2 + 1$, so that $m(i) = 0$.

Lemma 5.9. Every polynomial $a \in K[t]$ is congruent modulo m to a unique polynomial of degree $< \delta m$.

Proof. Divide a/m with remainder, $a = qm + r$, with $q, r \in K[t]$ and $\delta r < \delta m$. Then, $a - r = qm$, so $a \equiv r \pmod{m}$.

It remains to prove uniqueness.

Suppose $\exists\ r \equiv s \pmod{m}$, with $\delta r, \delta s < \delta m$. Then, $r - s$ is divisible by m, but has smaller degree than m.

Therefore, $r - s = 0$, so $r = s$, proving uniqueness. $\square$

Lemma 5.14. Let $K(\alpha) : K$ be a simple algebraic extension, let m be the minimal polynomial of α over K, let $\delta m = n$.

Then $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a basis for $K(\alpha)$ over K. In particular, $[K(\alpha) : K] = n$.

Definition 6.2. The degree $[L : K]$ of a field extension $L : K$ is the dimension of L considered as a vector space over K.

Equivalently, the dimension of L as a vector space over K is the number of terms in the expression for a general element of L using coefficients from K.

Example 6.3.

1. $\mathbb{C}$ elements are 2-dimensional over $\mathbb{R}$ ($p + qi \in \mathbb{C}$, with $p, q \in \mathbb{R}$), because a basis is $\{1, i\}$, hence $[\mathbb{C} : \mathbb{R}] = 2$.
2. $[\mathbb{Q}(i, \sqrt{5}) : \mathbb{Q}] = 4$, since the elements $\{1, \sqrt{5}, i, i\sqrt{5}\}$ form a basis for $\mathbb{Q}(i, \sqrt{5})$ over $\mathbb{Q}$.

Theorem 6.4. *(Short Tower Law)* If $K, L, M \subseteq \mathbb{C}$, and $K \subseteq L \subseteq M$, then $[M : K] = [M : L] \cdot [L : K]$.

Proof. Let $(x_i)_{i \in I}$ be a basis for L over K, let $(y_j)_{j \in J}$ be a basis for M over L. $\forall i \in I, j \in J$, we have $x_i \in L, u_j \in M$.
Want to show that $(x_i y_j)_{i \in I, j \in J}$ is a basis for M over K.

i. prove linear independence:
Suppose that

$$\sum_{ij} k_{ij} x_i y_j = 0 \; (k_{ij} \in K)$$

rearrange

$$\sum_j (\underbrace{\sum_i k_{ij} x_i}_{\in L}) y_j = 0 \; (k_{ij} \in K)$$

Since $\sum_i k_{ij} x_i \in L$, and the $y_j \in M$ are linearly independent over L, then $\sum_i k_{ij} x_i = 0$.
Repeating the argument inside $L \longrightarrow k_{ij} = 0 \;\; \forall i \in I, j \in J$.
So the elements $x_i y_j$ are linearly independent over K.

ii. prove that $x_i y_j$ span M over K:
Any $x \in M$ can be written $x = \sum_j \lambda_j y_j$ for $\lambda_j \in L$, because y_j spans M over L. Similarly, $\forall j \in J, \; \lambda_j = \sum_i \lambda_{ij} x_i y_j$ for $\lambda_{ij} \in K$.
Putting the pieces together, $x = \sum_{ij} \lambda_{ij} x_i y_j$ as required.

$\square$

Lemma 6.6. *(Tower Law)*
If $K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n$ are subfields of $\mathbb{C}$, then

$$[K_n : K_0] = [K_n : K_{n-1}] \cdot [K_{n-1} : K_{n-2}] \cdot \ldots \cdot [K_1 : K_0]$$

References

[1] Ian Stewart. Galois Theory, Third Edition, 2004.