Introduction to Algebra

Lecture Notes in the Winter Semester 2018/19

CONTENTS

INTRODUCTION

These are my personal lecture notes for the lecture *Introduction to Algebra* held by Prof. Dr. Jan Schröer at the University of Bonn in the winter term 2018/19.

I try to update them on my website, `https://pankratius.github.io`.
The authors labels his own comments and additions in purple.

The book [Alu09] is used by the author for further references, and highly recommended.

I will write them in English, as Prof. Schroer already provides a german version of his lecture notes. In addition, the first two lectures are ommited, as they were only motivational, but my motivation to draw a lot of pictures is fairly limited.

3.1 Algebraic Field Extensions

Let L/K be a field extension.

Recall from lecture 1:

Definition 3.1.1. L/K is called **extension by radicals**, if

i) There are finitely many $x_1, ..., x_n \in L$, such that

$$L = K(x_1, ..., x_n);$$

ii) there are $r_1, ..., r_n \geq 1$, such that

$$x^{r_1} \in K \text{ and } x_i^{r_i} \in K(x_1, ...x_{i-1}) \text{ for } 2 \leq i \leq n.$$

Definition 3.1.2. An element $x \in L$ is called **algebraic! element of a field extension** over K, if there is a non-zero polynomial $0 \neq f \in K[X]$, such that $f(x) = 0$. Otherwise, x is called **transcendental**.

Example 3.1.3. i) Consider $\mathbb{C}/\mathbb{Q}$. Then the n-th roots of unity $\rho_n^k := \exp(2\pi i/n)^k$ are algebraic over $\mathbb{Q}$, as they are the roots of $X^n - 1$.

ii) $\sqrt[3]{2}$ is an albraic over $\mathbb{Q}$ (for $\mathbb{C}/\mathbb{Q}$), as it is a root of $X^3 - 2$.

Proposition 3.1.4. *Consider $\mathbb{C}/\mathbb{Q}$. Then there are only countably many $x \in \mathbb{C}$ that are algebraic over $\mathbb{Q}$.*

Proof. The rationals are countable, and hence so is $\mathbb{Q}^n$.
There is a bijection

$$\mathbb{Q}^n \longleftrightarrow \{\text{polynomials of degree } \leq n-1\},$$

so

$$\mathbb{Q}[x] = \bigcup_{n \in \mathbb{N}} \{\text{polynomials of degree } \leq n-1\}$$

is countable. Since any polynomial in $\mathbb{Q}[X]$ has only finitely many roots, the assertion follows. □

Proposition 3.1.5. *Let $x \in L$ be algebraic over K. Then there is a uniquely determined irreducible and normend polynomial f in $K[X]$, such that $f(x) = 0$.*

Proof. This is supposed to be the same as in LA2. □

This polynomial is called the **minimal polynomial of** x **over** K and is denoted by $\mu_{x,K}$. Its degree is denoted by

$$[x : K] := \deg \mu_{x,K}$$

and is called the **degree of** x **over** K . For $x \in L$ transcendental, we set

$$[x : K] := \infty \text{ and } 0 := \mu_{x,K}.$$

Example 3.1.6. i) For $a \in L$, the following are equivalent:

i) $a \in K$

ii) $[a, K] = 1$

iii) $\mu_{x,K} = X - a$

ii) Since $i \in \mathbb{C} \setminus \mathbb{R}$, we have $[i : \mathbb{R}] \geq 2$. On the other hand, for $f \in \mathbb{R}[X], f := X^2 + 1$, $f(i) = 0$ holds. So $[i, \mathbb{R}] = 2$ and $\mu_{i,\mathbb{R}} = X^2 + 1$.

Definition 3.1.7. A field extension L/K is called **algebraic** , if all $x \in L$ are algebraic over K. Otherwise, L/K is called **transcendental** .

Example 3.1.8. $\mathbb{C}/\mathbb{Q}$ and $\mathbb{R}/\mathbb{Q}$ are both transcendental field extensions.

For a field extension L/K, L has the structure of a K-vector space, given by the restriction of the multiplication. The dimension of L as a K-vector space is denoted by

$$[L : K] := \dim_K L.$$

We say that L/K is a **finite** field extension , if $[L : K] < \infty$.

Lemma 3.1.9. *Let L/K be a finite. Then:*

i) L/K is algebraic.

ii) For all $x \in L$, $[x : K] \leq [L : K]$.

Proof. Let $[L : K] := n$ and $x \in L$ be arbitrary. Then the vector system

$$(1, x, ..., x^n)$$

is linear dependent, so there are $\lambda_0, ..., \lambda_n \in K$, such that

$$\lambda_0 + \lambda_1 x + ... + \lambda_n x^n = 0.$$

Therefor, for the polynomial

$$p := \lambda_0 + ... + \lambda_n X^n \in K[X]$$

the relation

$$p(x) = 0$$

holds. So L/K is algebraic, and $[x : K] \leq [L : K]$, as $\deg \mu_{x,K} \leq \deg p$. □

Theorem 3.1.10. *Let $L = K(x)$ be a field extension. Then*
$$[x : K] = [L : K].$$

Proof. Assume that x is transcendental over K. Then lemma 3.1.9 implies that $[L : K] = \infty$, and by definition $[x : K] = \infty$.

Assume that x is algebraic over K, and set $n := [x : K]$, $f := \mu_{x,K}$. Then the vector system
$$(1, ..., x^{n-1})$$
is linearly independent (otherwise there would be a polynomial of degree $n-1$ which anihilates x). Set
$$\tilde{K} := K + Kx + ... + Kx^{n-1},$$
which is a K-subspace of L. As $(1, ..., x^{n-1})$ is linearly independent, it is a basis of $\tilde{K}$, and hence $\dim_K \tilde{K} = n$. We now show that $\tilde{K}$ is also a subfield of L: As $\tilde{K}$ is a K-subspace of L, it is a additive subgroup of $(L, +)$.

$\tilde{K}$ is closed under multiplication: It suffices to show that for all $1 \leq i, j \leq n-1$ $x^i \cdot x^j \in \tilde{K}$, as elements in $\tilde{K}$ are linear combinations of scalar multiples of x^i for $0 \leq i \leq j$. Consider now the polynomial $X^{i+j} \in K[X]$. Euclidean division gives polynomials $q, r \in K[X]$, such that
$$X^{i+j} = qf + r, \tag{$*$}$$
with $\deg r \leq \deg f = n - 1$. So there are $b_0, ..., b_{n-1} \in K$, such that
$$r = b_0 + b_1 X + ... + b_{n-1} X^{n-1} A \in K[X].$$
Evaluating ($*$) at x, we get
$$x^{i+j} = r(x) = b_0 + ... + b_{n-1} x^{n-1},$$
since $f(x) = 0$. But this implies that $x^{i+j} \in \tilde{K}$.

$\tilde{K}$ is closed under inversion: Let $0 \neq y \in \tilde{K}$. As $\dim_K \tilde{K} = n$, y is algebraic over K. Let
$$\mu_{y,K} = X^m + ... + c_0.$$
Then $c_0 \neq 0$, as $\mu_{y,K}$ is irreducible. Rearanging, we get
$$1 = y \left(\frac{-c_1}{c_0} + \frac{-c_2}{c_0} y + ... + \frac{-c_n}{c_0} y^{n-1} \right),$$
so
$$y^{-1} = y \left(\frac{-c_1}{c_0} + \frac{-c_2}{c_0} y + ... + \frac{-c_n}{c_0} y^{m-1} \right) \in \tilde{K},$$
as $\tilde{K}$ is closed under addition and multiplication.

This shows that $\tilde{K}$ is a subfield of $K(x)$. But as $K(x)$ is the inclusion minimal field extension of K, this implies $\tilde{K} = K(x)$. But
$$\dim_K(\tilde{K}) = [x : K],$$
which concludes the proof. □

Corollary 3.1.11. *Let $x \in L$, such that $[x : K] = n$. Then*

i) Then $K(x)/K$ is finite and algebraic.

ii) $[K(x) : K] = n$

iii) $\{1, ..., x^{n-1}\}$ is a basis of $\tilde{K}$.

Proof. Consider the field extension $K(x)/K$, then apply theorem theorem 3.1.10, and i) follows from lemma 3.1.9. □

Example 3.1.12. i) $[\mathbb{R}, \mathbb{Q}] = \infty$.

ii) $[\mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}] \leq 3$, as $\mu_{\sqrt[3]{2},\mathbb{Q}} \mid (X^3 - 2)$

iii) Let ρ be a n-th root of unity, then

$$[\mathbb{Q}(\rho), \mathbb{Q}] \leq n - 1,$$

as

$$X^n - 1 = (X - 1)(X^{n-1} + ... + X + 1).$$

iv) Consider $\mathbb{C}/\mathbb{R}$. Then

$$[\mathbb{R}(x), \mathbb{R}] = \begin{cases} 1, & \text{if } x \in \mathbb{R} \\ 2, & \text{else} \end{cases}.$$

Definition 3.1.13. A subfield $Z \subset L$ is called an **intermediate field** of L/K, if

$$K \subseteq Z \subseteq L.$$

Theorem 3.1.14 (degree formular). *Let Z be an indermediate field of L/K. Then*

$$[L : K] = [L : Z][Z : K].$$

Proof. Assume $[L : Z] = r$ and $[Z : K] = s$, with $r, s \in \mathbb{N}$. Let $(w_1, ..., w_r)$ be a basis of L/Z and $(v_1, ..., v_r)$ a basis of Z/K. Now, let

$$y = \lambda_1 w_1 + ... + \lambda_r w_r \in L \text{ with } \lambda_i n Z \text{ and } w_1, ..., w_r \in L.$$

But since $\lambda_i \in Z$, there are $\mu_{i,1}, ..., \mu_{i,s} \in K$ such that

$$\lambda_i = \mu_{i,1} v_1 + ... + \mu_{i,s} v_s.$$

So

$$y = \sum_{\substack{1 \leq i \leq r \\ 1 \leq j \leq s}} \mu_{ij} v_j w_i,$$

and hence

$$\{w_i v_j \mid 1 \leq i \leq r, 1 \leq j \leq s\}$$

is a system of generators of L/K. Assume that

$$0 = \sum_{\substack{1\le i\le r\\ 1\le j\le s}} \mu_{ij} v_j w_i \implies \sum_{j=1}^{r} \alpha_{i,j} v_j = 0 \implies \alpha_{i,j} = 0,$$

as both the w_i and the v_j are linearly independent. This shows that the $w_i v_j$ are a basis of L/K.

Assume that $[L:Z] = \infty$ or $[Z:K] = \infty$. This already implies $[L:K] = \infty$.

□

Corollary 3.1.15. *Let L/K be finite. Then $[x:K]$ divides $[L:K]$ for all $x \in K$.*

Proof. Use $[x:K] = [K(x):K]$ and $[L:K] = [L:K(x)][K(x):L]$. □

Theorem 3.1.16. *Let L/K be a field extension. The following are equivalent:*

i) L/K is finite.

ii) L/K is algebraic, and there are $x_1, ..., x_n \in L$, such that

$$L = K(x_1, ..., x_n)$$

iii) There are $x_1, ..., x_n \in L$ such that

$$L = K(x_1, ..., x_n)$$

and x_1 is algebraic over K, x_i is algebraic over $K(x_1, ..., x_{i-1})$ for $2 \le i \le n$.

Proof. i) $\implies$ ii): As $[L:K] < \infty$, theorem 3.1.14 implies $[x:K] < \infty$, for all $x \in L$, so L/K is algebraic. Assume now there is a $x_1 \in L \setminus K$. Then

$$n_1 := [K(x_1):K] \ge 2$$

. If there is another $x_2 \in L/K(x_1)$, then

$$n_2 := [K(x_1, x_2) : K(x_2)] \implies n_1 n_2 > n_1.$$

Continuing inductivley, this has to stop after finitely many x_i, as $[L:K]$ is finite.

ii) $\implies$ iii): clear.

iii) $\implies$ i): Let $L = K(x_1, ..., x_n)$. Set

$$K_0 := K, ..., K_i := K(x_1, ..., x_i).$$

As x_i is algebraic over K_{i-1}, this implies

$$[K_i : K_{i-1}] < \infty.$$

Continuing inductivley, theorem 3.1.14 implies

$$[L : K] = \prod_{i=1}^{n} n_i < \infty.$$

$\square$

End of Lecture 3

A.1 Sheet 1

Proposition A.1.1. *Let $\alpha : R \to S$ be a homomorphism of commutative rings, and $s \in S$ arbitrary. Then there is a unique ring homomorphism $\overline{\alpha} : R[x] \to S$ extending α and sending $x \to s$:*

$$\begin{tikzcd} R \arrow[r, "\alpha"] \arrow[d] & S \\ R[x] \arrow[ur, dashed, "\overline{\alpha}"'] & \end{tikzcd}$$

Corollary A.1.2. *Let $n \in \mathbb{N}$. Then there is a ring homomorphism $\mathbb{Z}[x] \to \mathbb{Z}/n\mathbb{Z}[x, y]$:*

$$\begin{tikzcd} \mathbb{Z} \arrow[r, two heads] \arrow[d] & \mathbb{Z}/n\mathbb{Z} \arrow[r, hook] & \mathbb{Z}/n\mathbb{Z}[x] \arrow[r, hook] & \mathbb{Z}/n\mathbb{Z}[x,y] \\ \mathbb{Z}[x] \arrow[urrr, dashed, bend right] & & & \end{tikzcd}.$$

[Alu09] Paolo Aluffi. **Algebra: chapter 0**. Vol. 104. American Mathematical Soc., 2009.