Algebra I

Nicholas Schwab

Sommersemester 2017

1. The Hilbert Basis- and Nullstellensatz

1.1. Noetherian Rings

Definition 1. Let R be a ring, and $f_1, \dots, f_n \in R$, then the *ideal generated by the f_i* is

$$(f_1, \dots, f_n)_R = \left\{ \sum \lambda_i f_i \;\middle|\; \lambda_i \in R \right\} = \bigcap_{f_1, \dots, f_n \in I \text{ ideal}} I \,.$$

The f_i are called a *basis* or *generators* of I.

Remark 1. If I is not necessarily finite,

$$(f_i \mid i \in I)_R = \left\{ \sum_{i \in I} \lambda_i f_i \;\middle|\; \lambda_i = 0 \text{ for all but finitely many } i \right\} = \bigcap_{(f_i)_{i \in I} \subseteq I} I \,.$$

Definition 2. Let k be a field, $I \subseteq k[X_1, \dots, X_n]$ an ideal, ℓ a field extension of k. Call $x \in \ell^n$ a *zero* of I iff $f(x_1, \dots, x_n) = 0$ for all $f \in I$.

Remark 2. An element x is a common zero of the $f_i \in k[X_1, \dots, X_n]$ iff it is a zero of the ideal generated by the f_i.

Proposition 1. *For a ring R the following conditions are equivalent:*

(i) *Every ideal has a finite set of generators (i.e. is finitely generated).*

(ii) *Every ascending chain $I_0 \subseteq I_1 \subseteq \dots$ of ideals in R terminates after finitely many steps, i.e. there is some $N \in \mathbb{N}$ such that $I_n = I_N$ for all $n \geq N$.*

(iii) *Every non-empty set $\mathfrak{M}$ of ideals in R has an $\subseteq$-maximal element I.*

Definition 3. A ring with these properties is called *Noetherian.*

Example 1. Fields and principal ideal domains are Noetherian.

Theorem 1 (Hilbert's Basissatz)**.** *If R is Noetherian, so is $R[X_1, \dots, X_n]$.*

Corollary 1 (of the Basissatz)**.** *Every polynomial system of equations in finitely many variables over a field has finite subsystem with the same set of solutions.*

Theorem 2 (Hilbert's Nullstellensatz)**.** *Let k be a algebraically closed field and I be a proper ideal of $k[X_1, \dots, X_n]$. Then I has a zero $x \in k^n$.*

Both Hilbert's Nullstellensatz and Hilbert's Basissatz will be proved later on.

1.2. Modules over rings

Definition 1. An R-Module (where R is a ring) is an abelian group $(M, +)$ with an operation

$$\cdot : R \times M \longrightarrow M \;, \quad (r, m) \longmapsto r \cdot m$$

such that for all $r, s \in R$ and $m, n \in M$

$$\begin{aligned} r \cdot (s \cdot m) &= (r \cdot s) \cdot m & \qquad (r + s) \cdot m &= r \cdot m + s \cdot m \\ 1 \cdot m &= m & r \cdot (m + n) &= r \cdot m + r \cdot n \;. \end{aligned}$$

A *morphism* of R-Modules is a map $M \xrightarrow{f} N$ which is a homomorphism of abelian groups compatible with $\cdot$. A *submodule* of M is a subgroup $X \subseteq M$ of $(M, +)$ such that $R \cdot X \subseteq X$.

Example 1. The R-submodules of R are the ideals in R.

Proposition 1. *If $N \subseteq M$ is a R-submodule of the R-module M the quotient group M/N has a unique structure of an R-submodule such that the projection $M \xrightarrow{\pi} M/N$ is a morphism of R-modules, and for arbitrary R-modules T the map*

$$\begin{aligned} \mathrm{Hom}_R(M/N, T) &\longrightarrow \{\tau \in \mathrm{Hom}_R(M, T) \mid \tau|_N = 0\} \\ t &\longmapsto \tau = t \circ \pi \end{aligned}$$

is bijective, where t is surjective iff τ is and t is injective iff $\ker(\tau)$ equals N.

Corollary 1. *Let $N, L \subseteq M$ be submodules of some R-Module M.*

(i) *There is a unique isomorphism $L/(N \cap L) \xrightarrow{\sim} (N + L)/N$ such that the following diagram commutes:*

$$\begin{tikzcd} L \arrow[r, hook] \arrow[d, "\pi_{L/(N\cap L)}"'] & N + L \arrow[d, "\pi_{(N+L)/N}"] \\ L/(N \cap L) \arrow[r, dashed, "\sim"] & (N + L)/N \end{tikzcd}$$

(ii) *If further $L \subseteq N$, there is a unique isomorphism $M/N \xrightarrow{\sim} (M/L)/(N/L)$ such that the following diagram commutes:*

$$\begin{tikzcd} M \arrow[r, "\pi_{M/L}"] \arrow[d, "\pi_{M/N}"'] & M/L \arrow[d, "\pi_{(M/L)/(N/L)}"] \\ M/N \arrow[r, dashed, "\sim"] & (M/L)/(N/L) \end{tikzcd}$$

Definition 2. If M and N are R-modules, $M \oplus N = M \times N$ equipped with component-by-component addition and scalar multiplication. This can be generalized to finitely many summands.

Example 2. $R^n = \{(r_i)_{i=1}^n \mid r_i \in R\}$ is an R-module.

Definition 3. If M is an R-module and $m_1, \ldots, m_k \in M$, then the *submodule generated by* $\{m_1, \ldots, m_k\}$ *is*

$$\langle m_1, \ldots, m_k \rangle_R = Rm_1 + \ldots + Rm_k = \left\{ \sum r_i \cdot m_i \;\middle|\; r_i \in R \right\} = \bigcap_{m_1,\ldots,m_k \in X \text{ submodule}} X$$

As was the case for Definition 1.1.1, this can be generalized to infinitely many generators. M is *finitely generated* iff there are $m_1, \ldots, m_k \in M$ such that the submodules of M generated by the m_i equals M.

Proposition 2. *Consider an exact sequence*

$$0 \longrightarrow N \longrightarrow M \longrightarrow L \longrightarrow 0$$

of R-modules.

(i) *If M is finitely generated, then so is L.*

(ii) *If N and L are finitely generated, then so is M.*

Corollary 2. *$M \oplus N$ is finitely generated iff M and N are.*

Proposition 3. *Let M be an R-module. The following properties are equivalent:*

(a) *Every submodule $N \subseteq M$ of M is finitely generated.*

(b) *Every ascending sequence $N_0 \subseteq N_1 \subseteq \ldots$ of submodules of N terminates.*

(c) *Every non-empty set $\mathfrak{M}$ of R-submodules of M has a $\subseteq$-maximal element.*

Proof. **(a)** $\rightarrow$ **(b)** Let $N_\infty = \bigcup_{i=0}^{\infty} N_i$, then this is a submodule, hence finitely generated by a). Let $n_1, \ldots, n_k$ generate N_∞. Choose ℓ_i such that $n_i \in N_{\ell_i}$ and let $\ell = \max_{i \leq k} \ell_i$, then $N_\ell = N_\infty$.

(b) $\rightarrow$ **(c)** From b) we conclude, that in the $\subseteq$-ordered set $\mathfrak{M}$ every ascending chain has an upper bound in $\mathfrak{M}$, namely the ideal, that terminates the chain. Therefore by Zorn's Lemma there is $\subseteq$-maximal element in $\mathfrak{M}$.

(c) $\rightarrow$ **(a)** Let $\mathfrak{M}$ be the set of finitely generated submodules of N. Since $\{0\} \subseteq N$ is a module, this set is not empty. Therefore there is a $\subseteq$-maximal submodule P in $\mathfrak{M}$ generated by $p_1, \ldots, p_n$. Therefore there is no $f \in N \setminus P$ such that $\langle p_1, \ldots, p_n, f \rangle_R$ is a submodule of N since this would be a superset of P. Hence we have $N = P$ is finitely generated.

$\square$

Definition 4. A module over a ring R is *Noetherian* iff the equivalent conditions above are fulfilled.

Remark 1. Sub- and quotient modules of Noetherian rings are Noetherian. If N is a submodule of M and if N and M/N are Noetherian, then M is Noetherian.

Proof. The first assertion follows easily from Proposition 2 and the characterization of *Noetherian modules* by Proposition 3(a). For the second assertion let N and M/N be Noetherian and $X \subseteq M$ be a submodule. Since both $(X \cap N) \subseteq N$ and $X/(X \cap N) \simeq (X + N)/N \subseteq M/N$ are finitely generated as submodules of N, M/N respectively, we obtain the exact sequence

$$0 \longrightarrow X \cap N \longrightarrow X \longrightarrow X/(X \cap N) \longrightarrow 0 \, ,$$

proving that X is finitely generated by Proposition 2. $\square$

Remark 2. Any Noetherian module is finitely generated.

Proposition 4. *Let R be a Noetherian ring. Then any finitely generated R-module is Noetherian.*

Proof. We proceed by induction on the number of generators of M. The case of only one generator is immediate. Now let $M = Rm_1 + \ldots + Rm_k$ and any Ry -module with less than k generators be Noetherian. In particular, $N = Rm_1 + \ldots + Rm_{k-1}$ is Noetherian. The map $R \to M/N$ sending $r \in R$ to $rm_k + N$ is surjective, hence M/N is isomorphic to some quotient of R and thus Noetherian by Remark 1. Then, again by Remark 1, M is Noetherian. $\square$

Definition 5. For a module M over a ring R, define

$$\mathrm{Ann}(M) = \{r \in R \mid r \cdot M = \{0\}\} = \{r \in R \mid r \cdot m = 0 \ \forall m \in M\} \, .$$

It is called the *annihilator* or *annulator* of M.

Proposition 5. *A module M over a ring R is Noetherian iff it is finitely generated and $R/\mathrm{Ann}(M)$ is a Noetherian ring.*

1.3. Proof of the Hilbert basis theorem

Proof. Let R be a Noetherian ring and $I \subseteq R[T]$ be an ideal. Let $R[T]_{\leq n}$ be the set of polynomials over R of degree smaller or equal to n. This is isomorphic to R^{n+1} ($1, \ldots, T^n$ being free generators) as R-modules, thus Noetherian (Proposition 1.2.4) which implies that $I_{\leq n} = I \cap R[T]_{\leq n}$ is a finitely generated R-module. Let I_n be the set of all $a_n \in R$, such that $a_0 + a_1 T + \ldots + a_n T^n \in I$ for some $a_0, \ldots, a_{n-1} \in R\}$. This is an ideal ($R$-submodule) of R, being the image of $I_{\leq n} \to R$ sending $a_0 + a_+ \ldots + a_n T^n \in I_{\leq n}$ to a_n. We have $I_n \subseteq I_{n+1}$ as $T \cdot I_{\leq n} \subseteq I_{\leq n+1}$. As R is Noetherian, this chain terminates at some $N \in \mathbb{N}$ with $I_n = I_N$ for $n \geq N$. Let $f_1, \ldots, f_k$ be generators of $I_{\leq N}$ as an R-module. We claim that they generate I as an $R[T]$-module. Since they generate $I_{\leq N}$ as an R-module, their N-th coefficients $f_N^{(i)}$, where $i \leq k$, generate $I_n = I_N$, for $n \geq N$, as an R-module.

We show by induction on n, that any $g \in I_{\leq n}$ belongs to $(f_1, \ldots, f_k)_{R[T]}$, thus establishing $I = (f_1, \ldots, f_k)_{R[T]}$. For $n \leq k$ we have $g \in I_{\leq N}$ and the assertion is obvious. Let $n > N$ let the assertion be valid for all $h \in I_{\leq n-1}$. Let $g = \sum_{i=1}^n g_i T^i$, $g_n = \sum_{i=1}^k \gamma_i f_N^{(i)}$ and $h = g - \sum_{i=1}^k \gamma_i T^{n-N} f_i$, then $h \in I_{\leq n-1}$ as the coefficient of T^n cancels. Thus, $h = \sum_{i=1}^k \rho_i f_i$ with $\rho_i \in R[T]$ by the induction assumption and

$$g = \sum_{i=1}^k (\gamma_i T^{n-k} + \rho_i) f_i \in (f_1, \ldots, f_k)_{R[T]}$$

as claimed. This shows that I is finitely $R[T]$-generated, hence $R[T]$ is Noetherian. $\square$

Corollary 1. *If R is a Noetherian ring, so is $R[X_1, \ldots, X_n]$ for all $n \in \mathbb{N}$.*

1.4. Finiteness properties of R-algebras

Definition 1. Let R be a ring. An *R-algebra* is a ring A (commutative, with 1) together with a ring homomorphism $R \xrightarrow{\alpha} A$. Then A becomes an R-module via $r \cdot a := \alpha(r) \cdot a$. We call A *finite over R* (or *finite as an R-algebra*) if it is finitely generated as an R-module. We call A of *finite type over R* if it is finitely generated as an R-algebra in the sense that there are $f_1, \ldots, f_k \in A$, $k \in \mathbb{N}$, such that any R-subalgebra $B \subseteq A$ (i.e. any subring $B \subseteq A$ which is also a R-submodule, or, equivalently, a subring containing the image of α) containing the f_i must equal A.

Remark 1. If A is an R-algebra and $f_1, \ldots, f_k \in A$, the following subsets of A coincide:

- $\left\{\sum r_\alpha f_1^{\alpha_1} \cdot \ldots \cdot f_k^{\alpha_k} \mid r_\alpha \in R, r_\alpha \neq 0 \text{ only for finitely many } \alpha\right\}$
- The image of the ring homomorphism $R[X_1, \ldots, X_k] \to A$ sending $p \in R[X_1, \ldots, X_k]$ to $p(f_1, \ldots, f_k)$.
- The intersection of all R-subalgebras of A containing the f_i.

Thus, an R-algebra A is of finite type iff it is isomorphic to a quotient of $R[X_1, \ldots, X_k]$ by some ideal I for finite k.

Remark 2. a) Obviously, if $f_1, \ldots, f_i \in A$ generate A as an R-module, they generate it as an R-algebra. Thus any finite R-algebra is of finite type. On the other side, when $R \neq \{0\}$ and and $n > 0$, $R[X_1, \ldots, X_n]$ is an R-algebra of finite type that is not finitely generated as an R-module.

b) Obviously, if L/K is a field extension then L is a finite K-algebra iff the field extension is finite. The fact that this still holds if L is a K-algebra of finite type turns out to be essentially equivalent to the Nullstellensatz.

Proposition 1. *Let R be a ring, A an R-algebra. Any A-algebra B becomes an R-algebra via the composition $R \to A \to B$.*

(i) *If A is finite over R, it is of finite type over R.*

(ii) *(transitivity of finiteness) If B is finite over A and A finite over R, then B is finite over R.*

(iii) *If B over A and A over R are of finite type, then B is of finite type over R.*

(iv) *An algebra of finite type over a Noetherian ring is a Noetherian ring.*

Proof. (i) Trivial.

(ii) If $b_1, \ldots, b_m$ generate B as an A-module and $a_1, \ldots, a_n$ generate A as an R-module, the $\beta_{i,j} = a_j \cdot b_i$ generate B as an R-module: Indeed, let $b \in B$, then $b = \sum_{i=1}^m \alpha_i b_i$ (with $\alpha_i \in A$) and each α_i can be written as $\alpha_i = \sum_{j=1}^n r_{i,j} a_j$. Then $b = \sum_{i=1}^m \sum_{j=1}^n r_{i,j} \beta_{i,j}$.

(iii) By Remark 1, we obtain surjective homomorphisms $A[Y_1, \ldots, Y_m] \xrightarrow{\beta} B$ (as A-algebras, hence also as R-algebras) and $R[X_1, \ldots, X_n] \xrightarrow{\alpha} A$ (as R-algebras). Lifting the latter to a surjective homomorphism $R[X_1, \ldots, X_n, Y_1, \ldots, Y_m] \to A[Y_1, \ldots, Y_m]$ and composing them provides us with a surjective homomorphism

$$R[X_1, \ldots, X_n, Y_1, \ldots, Y_m] \longrightarrow B\ ,$$

proving that B is of finite type over R. In particular, if $b_1, \ldots, b_m$ generate B as an A-algebra and $a_1, \ldots, a_n$ generate A as an R-algebra, then B is generated by $a_1, \ldots, a_n, b_1, \ldots, b_m$ as an R-algebra.

(iv) Note that the quotient of a Noetherian ring by an ideal stays Noetherian: The preimage of an infinitely ascending chain of ideals of the quotient ring would be an infinitely ascending chain of ideals of the original ring. Now if $a_1, \ldots, a_m \in A$ generate A as an R-algebra, then

$$\begin{aligned} R[X_1, \ldots, X_m] &\longrightarrow A \\ p &\longmapsto p(a_1, \ldots, a_m) \end{aligned}$$

is surjective and A is isomorphic to a quotient of $R[X_1, \ldots, X_m]$, which by the Basissatz is Noetherian if R is.

□

Proposition 2 (Artin-Tate)**.** *Let R be a Noetherian ring, A an R-algebra of finite type and $B \subseteq A$ an R-subalgebra such that A is finite over B. Then B is an R-algebra of finite type.*

Proof. Let $a_1, \ldots, a_m$ generate A as an R-algebra and let $\alpha_1, \ldots, \alpha_n$ generate it as a B-module. We have expressions

$$a_i = \sum_{j=1}^{n} b_{i,j}\alpha_j \quad \text{and} \quad \alpha_k \cdot \alpha_k = \sum_{j=1}^{n} \beta_{j,k,l}\alpha_j. \tag{$*$}$$

Let $\mathfrak{B} \subseteq B$ be the R-algebra generated by the $b_{i,j}$ and the $\beta_{j,k,l}$. It is of finite type over R thus Noetherian. Let $\mathfrak{A} \subseteq A$ be the $\mathfrak{B}$-submodule generated by $\alpha_1, \ldots, \alpha_n$. It is a subring containing the a_i by $(*)$ and is an R-algebra because $\mathfrak{B}$ is. Then $\mathfrak{A} = A$ and A is finite over $\mathfrak{B}$. Since $\mathfrak{B}$ is Noetherian, $B \subseteq A$ is a $\mathfrak{B}$-subalgebra, and B is finitely generated as $\mathfrak{B}$-module ($\mathfrak{B}$ being Noetherian), B is of finite type over $\mathfrak{B}$ (Proposition 1(i)) and thus also over R (Proposition 1(iii)). □

Proposition 3 (Eakin-Nagata)**.** *Let A be a Noetherian ring and $B \subseteq A$ be a subring such that A is finite over B. Then B is Noetherian.*

Remark 3. See Matsumura, CRT, for Eakin-Nagata.

1.5. The notion of integrity and the Noether Normalization Theorem

Remark of the author: It's called integrity not entireness...

Definition 1. Let $A \subseteq B$ be a ring extension. We call $b \in B$ *integral* over A if it satisfies an equation

$$b^n + a_{n-1}b^{n-1} + \ldots + a_1 b + a_0 = 0$$

with $a_0, \ldots, a_{n-1} \in A$. We call B over A *integral*, if every element of B is integral.

Remark 1. It is not really necessary to assume $A \to B$ to be injective.

Proposition 1. (i) *An element $b \in B$ is integral over A iff there is an intermediate ring $A \subseteq C \subseteq B$ containing b which is finite over A. If $b_1, \ldots, b_n$ are finitely many integral elements of B, there is an A-subalgebra $A \subseteq C \subseteq B$ containing all b_i which is finite over A.*

(ii) *The elements of B which are integral over A form a subring of B, the* integral closure *of A in B.*

(iii) *If C/B and B/A are integral, so is C/A.*

(iv) *Let B/A be integral (where it is essential that A is a subring of B). If B is a field, then so is A.*

Proof. (i) Let $b_1, \ldots, b_n$ be integral over A. Each b_i satisfies an equation

$$b_j^{d_i} = \sum_{i=0}^{d_i-1} a_{i,j} b_j^i \quad \text{where } a_{i,j} \in A\ .$$

Then the subring $C = A[b_1, \ldots, b_n]$ is generated by all $b_1^{k_1} \cdots b_n^{k_n}$ where $0 \le k_i < d_i$, hence it is finite over A. The first assertion of (i) follows as a special case.

For the other direction let $C \subseteq B$ be an A-subalgebra which is finitely generated as an A-module, say, by $\gamma_1, \ldots, \gamma_n$. Let $b \in C$ and choose $m_{i,j} \in A$ such that

$$b\gamma_j = \sum_{i=1}^{n} m_{i,j} \gamma_j$$

The matrix $M = (m_{i,j})_{i,j=1}^n$ satisfies its own characteristic equation by Cayley-Hamilton theorem: $M^n = p_0 + p_1 M + \ldots + p_{n-1} M^{n-1}$ for suitable $p_0, \ldots, p_{n-1} \in A$. Since b^j in C can be expressed by M^j (in the sense that

$$\begin{tikzcd}
(a_1, \ldots, a_n) \arrow[d, mapsto] & A^n \arrow[r, "M^j\cdot"] \arrow[d, "\gamma"'] & A^n \arrow[d, "\gamma"] & (a_1, \ldots, a_n) \arrow[d, mapsto] \\
\sum a_i \gamma_i & C \arrow[r, "\cdot b^j"] & C & \sum a_i \gamma_i
\end{tikzcd}$$

commutes) it follows, that $b^n \cdot c = p_0 c + p_1 bc + \ldots + p_{n-1} b^{n-1} c$ (first for $c = \gamma_i$, then all $c \in C$). Taking $c = 1$ shows that b is indeed integral over A.

(ii) If C is as in A and contains b_1, b_2, then it contains $b_1 \pm b_2$ and $b_1 \cdot b_2$, showing that these are integral over A.

(iii) Let, more generally, B/A be integral and $c \in C$ integral over B. It satisfies an equation $c^d = \beta_0 + \beta_1 c + \ldots + \beta_{d-1} c^{d-1}$ with $\beta_i \in B$. By (i), there is an A-subalgebra $\mathfrak{B} \subseteq B$ which is finite over A and contains the β_i. Then c is integral over $\mathfrak{B}$, hence by (i) there is a $\mathfrak{B}$-subalgebra $\mathfrak{C} \subseteq C$ containing c and finite over $\mathfrak{B}$. Now $\mathfrak{C}/A$ is finite by Proposition 1.4.1(ii), hence c is integral over A by (i).

(iv) Suppose that B is a field and let $a \in A \backslash \{0\}$. Since B/A is integral, we can find $\alpha_0, \ldots, \alpha_{n-1} \in A$ such that

$$\left(a^{-1}\right)^n + \sum_{i=0}^{n-1} \alpha_i \cdot \left(a^{-1}\right)^i = 0.$$

But then

$$a^{-1} = a^{n-1}\left(a^{-1}\right)^n = -\sum_{i=0}^{n-1} \alpha_i \cdot a^{n-1} \in A.$$

So every element of $A \setminus \{0\}$ is an unit and A a field.

$\square$

Remark 2. Cayley-Hamilton (similar to other determinant identities) can be derived from the case of algebraically closed fields by embedding integer domains into the algebraic closures of their quotient fields. Fir arbitrary rings R (possibly with zero divisors) one may consider the surjective ring homomorphism

$$\begin{aligned} \mathbb{Z}[X_r : r \in R] &\longrightarrow R \\ X_r &\longmapsto r \end{aligned}$$

and then reduce to the case of integer domains which was done above.

Corollary 1. *A ring extension is finite iff it is integral and of finite type.*

Remark 3. Algebraic independence over k means that

$$\sum_{\alpha \in \mathbb{N}^n} \lambda_{\alpha_1, \ldots, \alpha_n} a_1^{\alpha_1} \cdot \ldots \cdot a_n^{\alpha_n} = 0$$

implies that each $\lambda_{\alpha_1, \ldots, \alpha_n} = 0$. Equivalently, the ring homomorphism

$$\begin{aligned} k[X_1, \ldots, X_n] &\longrightarrow k[a_1, \ldots, a_n] \\ X_i &\longmapsto a_i \end{aligned}$$

is injective, hence $k[X_1, \ldots, X_n] \simeq k[a_1, \ldots, a_n]$ as k-algebras.

Theorem 1. *Let k be a field, A a k-algebra of finite type over k. Then there are over k algebraically independent $a_1, \ldots, a_n \in A$ such that $A/k[a_1, \ldots, a_n]$ is integral.*

Proof. Since A is of finite type over k, we can choose $a_1, \ldots, a_n$ such that A is integral over $k[a_1, \ldots, a_n]$ (e.g. choose the a_i as generators of A as k-algebra). We may choose a minimal n such that this is possible. We claim

$*$ Let $x_1, \ldots, x_n \in A$ such that A is integral over $k[x_1, \ldots, x_n]$ and n is minimal having this property that such x_i exist. Then the x_i are algebraically independent over k.

Write $x^\alpha = \prod_{i=1}^n x_i^{\alpha_i}$ for short. Suppose that

$$\sum_{\alpha \in \mathbb{N}_0^n} \lambda_\alpha \cdot x^\alpha = 0 \tag{\#}$$

where

$$S := \{\alpha \in \mathbb{N}_0^n | \lambda_\alpha \neq 0\}$$

is finite but not empty. Let $y_1 = x_1$ and $y_k = x_k + y_1^{d_k}$ (the d_i will be chosen later on). Since the x_i can be recovered from the y_i, we have $k[x_1, \dots, x_n] = k[y_1, \dots, y_n]$. The idea is to choose the d_i such that y_1 is integral over $k[y_2, \dots, y_n]$. Then A is integral over $k[y_2, \dots, y_n]$, contradicting the minimality of n.

Let $\omega_d(\alpha) = \alpha_1 + \sum_{i=2}^n d_i \cdot \alpha_i$. The summands can be expressed as

$$\begin{aligned} \lambda_\alpha x^\alpha &= \lambda_\alpha y_1^{\alpha_1} \cdot \prod_{i=2}^n \left(y_i - y_1^{d_i}\right)^{\alpha_i} \\ &= \pm \lambda_\alpha y_1^{\omega_d(\alpha)} + \sum_{j=0}^{\omega_d(\alpha)-1} Q_{\alpha,j}(y_2, \dots, y_n) y_1^j \end{aligned}$$

if all d_k are positive. Here $Q_{\alpha,j}$ denotes some polynomial.

If $d_2, \dots, d_n$ can be chosen in such a way that

$$\omega_d : S \longrightarrow \mathbb{N}$$

has a unique maximum $\alpha^* \in S$, the relation # becomes

$$0 = \lambda_{\alpha^*} y_1^{\omega_d(\alpha^*)} + \sum_{j=0}^{\omega_d(\alpha^*)-1} Q_j(y_2, \dots, y_n) y_1^j$$

proving, that y_1 is integral over $k[y_2, \dots, y_n]$.

Now $d_2, \dots, d_n$ can be chosen in several ways. For example, take

$$A = \max \{l \in \mathbb{N} : \text{ there is } \alpha \in S \text{ such that } l = \alpha_i \text{ for some } i\}$$

and chose $d_i = (A+1)^{i-1}$. Then ω_d is injective since the $(A+1)-$adic representation of an integer is unique. □

1.6. Proof of the Nullstellensatz and some consequences

Theorem 1. *Let L/K be a field extension such that L is a K-algebra of finite type. Then L/K is finite.*

Proof. By Noether's Normalization Theorem (Theorem 1.5.1) there are $y_1, \dots, y_n \in L$ algebraically independent over K such that L is integral over $K[y_1, \dots, y_n]$. By Proposition d), $K[y_1, \dots, y_n]$ is a field. But as $y_1, \dots, y_n$ are algebraically independent, $K[y_1, \dots, y_n]$ is isomorphic to the polynomial ring $K[X_1, \dots, X_n]$, which is only a field for $n = 0$. Thus L/K is integral (i.e. algebraic) and since the extension is finitely generated it must be finite. □

Remark 1. When K is uncountable and $\lambda \in L$ non-algebraic over K, the subfield $K(\lambda)$ is isomorphic to $K(X)$, the field of rational functions over K, which has uncountable dimension as a K-vector space as the $\frac{1}{X-\gamma}$, $\gamma \in K$, are linearly independent. But the dimension (as a K-vector space) of a K-algebra must be countable, as there are only countable many monomials in finitely many elements.

Corollary 1. *Let k be a field and let $\mathfrak{m} \subseteq k[X_1, \ldots, X_n]$ a maximal ideal, then it's residue field $k[X_1, \ldots, X_n]/\mathfrak{m}$ is a finite field extension of k.*

Proof. Indeed, it is generated by $X_1 + \mathfrak{m}, \ldots, X_n + \mathfrak{m}$ and thus finite over k. □

Remark 2. In particular, it L/K is algebraic and $L = K$ if L is algebraically closed.

Remark 3.

- A ring R is a *domain* if $0 \neq 1$ and from $a \cdot b = 0$ follows $a = 0$ or $b = 0$.
- A field is a domain in which every $x \neq 0$ is invertible.
- An ideal $\mathfrak{p} \subseteq R$ is a *prime ideal*, iff $1 \notin \mathfrak{p}$ and $ab \in \mathfrak{p}$ implies $a \in \mathfrak{p}$ or $b \in \mathfrak{p}$. This is equivalent to $R/\mathfrak{p}$ being a domain.

  It is *maximal* if $\mathfrak{p} \subsetneq R$ and there is not ideal I with $\mathfrak{p} \subsetneq I \subsetneq R$. This is equivalent to $R/\mathfrak{p}$ being a field.
- An element $p \in R$ of a domain is called *prime* if $p \neq 0$ and $p \cdot R$ is a prime ideal.

  It is called *irreducible* if $p \notin R^\times$ and $p = ab$ implies $a \in R^\times$ or $b \in R^\times$.

Theorem 2. *If $I \subsetneq k[X_1, \ldots, X_n]$ is a proper ideal in the polynomial ring over a field, it has a zero in l^n where l/k is some finite field extension. In particular, when k is algebraically closed, it has a zero in k^n.*

Proof. Let $\mathfrak{m} \supseteq I$ be a maximal ideal of $R = k[X_1, \ldots, X_n]$ and $l = R/\mathfrak{m}$. It is finite because of Corollary 1. Let $x_i \in l$ be the image of $X_i \in R$ under $R \longrightarrow R/\mathfrak{m}$. Then $(x_1, \ldots, x_n)$ is a zero of I in l^n. □

Proposition 1. *If k is algebraically closed, there is a bijection between k^n and maximal ideals $\mathfrak{m} \subset k[X_1, \ldots, X_n] =: R$*

$$\begin{aligned} x \in k^n &\longmapsto \mathfrak{m}_x = \{f \in R \mid f(x) = 0\} \\ \text{the only zero of } \mathfrak{m} &\longleftarrow\!\shortmid \mathfrak{m} \end{aligned}$$

Proof. Obviously, $\mathfrak{m}_x$ is an ideal and

$$\begin{aligned} R/\mathfrak{m}_x &\longrightarrow k \\ (f \mod \mathfrak{m}_x) &\longmapsto f(x) \end{aligned}$$

is an isomorphism. Thus $R/\mathfrak{m}_x$ is a field and $\mathfrak{m}_x$ is a maximal ideal. Moreover x is the only zero of $\mathfrak{m}_x$: If ξ is a different zero (say $\xi_i \neq x_i$), then $f(\xi) \neq 0$ for $f(X) = X_i - x_i$.

Let $\mathfrak{m}$ be any maximal ideal and x a zero of $\mathfrak{m}$, then $\mathfrak{m} \subseteq \mathfrak{m}_x$, hence $\mathfrak{m} = \mathfrak{m}_x$ by its maximality. By the previous remark x is the only zero of $\mathfrak{m}$. □

Remark 4. (a) If $k \neq \overline{k}$, the bijection is between $\mathrm{Aut}(\overline{k}/k)-$orbits on $\overline{k}^n$ and maximal ideals in $R = k[X_1, \ldots, X_n]$. If k has no separable extensions (i.e., k is *separably closed*, $k = k^{\mathrm{sep}}$), then the bijection is between $\overline{k}^n$ and $\mathfrak{m} - \mathrm{Spec}(R)$, the set of maximal ideals of R.

(b) For arbitrary R, Grothendieck takes arbitrary prime ideals (which the lecturer thinks was also proposed by Krull, who was a noob compared to Grothendieck) and turns $\mathrm{Spec}\, R$, the set of prime ideals of R, into a geometric object.

1.7. Some operations on ideals

Definition 1. For $k = \overline{k}$ and $I \subseteq R = k[X_1, \ldots, X_n]$ we denote the of zeros of I by $V(I)$ called the *variety* of I. If $I = \langle f_1, \ldots, f_k \rangle_R$ we write $V(f_1, \ldots, f_k)$ for $V(I)$.

Remark 1. By definition, $I \supseteq J$ implies $V(I) \subseteq V(J)$.

Definition 2. For ideals I, J of R let $I + J = \{f + g \mid f \in I, g \in J\}$. Here, R may be any ring.

Remark 2. For $R = k[X_1, \ldots, X_n]$ we have $V(I + J) = V(I) \cap V(J)$.

Definition 3. We can sum arbitrary many summands:

$$\sum_{\lambda \in \Lambda} I_\lambda = \left\{ \sum_{\lambda \in \Lambda} i_\lambda \;\middle|\; i_\lambda \neq 0 \text{ only for finitely many } \lambda \right\}$$

Remark 3. If $R = k[X_1, \ldots, X_n]$ then

$$V\left(\sum_{\lambda \in \Lambda} I_\lambda\right) = \bigcap_{\lambda \in \Lambda} V(I_\lambda)$$

Definition 4.

$$I \cdot J = \left\{ \sum_{k=1}^{n} f_k \cdot g_k \;\middle|\; f_k \in I, g_k \in J \right\}$$

Remark 4. If $R = k[X_1, \ldots, X_n]$ then $V(I \cdot J) = V(I \cap J) = V(I) \cup V(J)$.

Proof. By Remark 1

$$V(I \cdot J) \supseteq V(I \cap J) \supseteq V(I).$$

Thus

$$V(I) \cap V(J) \subseteq V(I \cap J) \subseteq V(I \cdot J)$$

and the latter is $\subseteq V(I) \cup V(J)$, implying equality. Indeed, let $x \in k^n \setminus (V(I) \cup V(J))$. Then there are are $f \in I$, $g \in J$ with $f(x) \neq 0$ and $g(x) \neq 0$. Then $f \cdot g \in (I \cdot J)$ and $(f \cdot g)(x) \neq 0$. $\square$

Remark 5. For infinite intersections the inclusion

$$\bigcup_{\lambda \in \Lambda} V(I_\lambda) \subseteq V\left(\bigcap_{\lambda \in \Lambda} I_\lambda\right)$$

may be proper.

Definition 5.

$$\sqrt{I} = \{f \in R \mid f^n \in I \text{ for some } n \in \mathbb{N}\} = \{f \in R \mid \text{the image of } f \text{ in } R/I \text{ is nilpotent }\}$$

Remark. (a) The set $\sqrt{\{0\}}$ of the nilpotent elements of R is called the *nil-radical* of R.

(b) If $f \in \sqrt{I}$, $g \in \sqrt{I}$ then $f^k \in I$ and $g^l \in I$ for $k, l \in \mathbb{N}$ then

$$(f+g)^{k+l} = \sum_{i+j=k+l} \binom{k+l}{i} f^i \cdot g^j \in I$$

(c) $\sqrt{\sqrt{I}} = \sqrt{I}$

Proposition 1. *If $k = \overline{k}$ and I and ideal in $R = k[X_1, \dots, X_n]$ then $\sqrt{I} = \{f \in R \mid f(x) = 0$ for all $x \in V(I)\}$.*

Proof. Is is clear that an element of $\sqrt{I}$ must vanish at all zeros of I. Conversely, let f vanish on $V(I)$. Consider the ideal $J \subseteq S = k[X_1, \dots, X_n, T]$ generated by the elements of I and by $g(X_1, \dots, X_n, T) = 1 - T \cdot f(X_1, \dots, X_n)$. If $(x, t) = (x_1, \dots, x_n, t)$ was a zero of J, x would be a zero of I, thus $f(x) = 0$, thus $g(x, t) = 1 - t \cdot f(x) = 1 \neq 0$, a contradiction. By the Nullstellensatz $J = S$. $\square$