Algebra I

Nicholas Schwab

Sommersemester 2017

1 The Hilbert Basis- and Nullstellensatz

1.1 Noetherian Rings

Definition 1.1.1. Let R be a ring, and $f_1, \ldots, f_n \in R$, then

$$\langle f_1, \ldots, f_n \rangle_R = \left\{ \sum_{i=1}^{n} \lambda_i f_i \middle| \lambda_i \in R \right\} = \bigcap_{\substack{I \subseteq R, \\ I \text{ ideal} \\ f_i \in I \forall i}}, I.$$

This is called the *ideal* generated by the f_i and the f_i are called a *basis* or *generators* of I.

Remark 1.1.1. If I is not necessarily finite,

$$\langle f_i \mid i \in I \rangle_R = \left\{ \sum_{i \in I} \lambda_i f_i \middle| \lambda_i = 0 \text{ for all but finitely many } i \right\} = \bigcap_{\substack{I \subseteq R, \\ I \text{ ideal} \\ f_i \in I \forall i}}, I.$$

Definition 1.1.2. Let k be a field, $I \subseteq k[T_1, \ldots, T_n]$ an ideal, l a field extension of k. $x \in l^n$ is a zero of I iff $f(x_1, \ldots, x_n) = 0$ for all $f \in I$.

Remark 1.1.2. x is a common zero of the $f_i \in k[X_1, \ldots, X_n]$ iff is a zero of the ideal generated by the f_i.

Proposition 1.1.1. *For a ring R the following conditions are equivalent:*

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

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

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

Definition 1.1.3. A ring with these properties is called *Noetherian.*

Example 1.1.1. Fields and principal ideal domains are Noetherian.

Theorem 1.1.1 (Hilbert's Basissatz)**.** *If R is Noetherian, $R[T_1, \ldots, T_n]$ (with finite n!) is Noetherian.*

Proof. The proof is recapitulated later on. $\square$

Corollary 1.1.1 (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 1.1.2 (Hilbert's Nullstellensatz). *Let k be a algebraically closed field and I be a proper ideal of $k[X_1, \ldots, X_n]$. Then I has a zero $x \in k^n$.*

Proof. This will be proofed in a few days. □

1.2 Modules over rings

Definition 1.2.1. An R-Module (where R is a ring) is an abelian group $(M, +)$ with an operation

$$\begin{aligned} \cdot : R \times M &\longrightarrow M \\ (r, m) &\longmapsto r \cdot m \end{aligned}$$

such that

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

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 1.2.1. The R-submodules of R are the ideals in R.

Proposition 1.2.1. *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*

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

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

Remark 1.2.1. Two important corollaries are:

$$(M/L)/(N/L) \xleftarrow{\simeq} M/N$$

for $M \supseteq N \supseteq L$ and, for submodules N and L of M

$$(N + L)/N \xleftarrow{\simeq} L/(N \cap L)$$

where $N + L$ denotes the submodule $\{l + n | l \in L, n \in N\}$ of M.

Definition 1.2.2. If M and N are R-modules, $M \oplus N = \{(m, n), | m \in M, n \in N\} = M \times N$ equipped with component-by-component addition and scalar multiplication. This can be generalized to finitely many summands.

Example 1.2.2. $R^n = \{(r_i)_{i=1}^n | r_i \in R\}$ is an R-module.

Definition 1.2.3. If M is an R-module and $m_1, \ldots, m_k \in M$, then the submodule generated by $\{m_i | 1 \leq i \leq k\}$ is

$$\left\{ \sum_{i=1}^{k} r_i \cdot m_i \middle| r_i \in R \right\} = \bigcap_{\substack{X \subseteq M \\ X \text{ module} \\ \text{all } m_i \in X}} X$$

As was the case for Definition 1.1.1, this can be generalized to infinitely many generators. M is finitely generated iff there are $(m_i)_{i=1}^{k}$, $k \in \mathbb{N}$, $m_i \in M$ such that the submodules of M generated by the m_i equals M.

Proposition 1.2.2. *Let $N \subseteq M$ be an R-submodule*

a) If M is finitely generated, M/N is finitely generated.

b) If N and M/N are finitely generated, M is finitely generated.

Corollary 1.2.1. *$M \oplus N$ is finitely generated iff M and N are. (Note that: $M \simeq M \oplus \{0\}$ and $(M \oplus N)/M \simeq N$)*

Proposition 1.2.3. *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)** $\to$ **b)** Let $N_\infty = \bigcup_{i=0}^{\infty} N_i$, then this is a submodule, hence finitely generated by a). Let $n_1, \ldots, n_k$, $k \in \mathbb{N}$, generate N_∞ and let j_i, for $1 \leq i \leq k$, be chosen such that $n_i \in N_{j_i}$ and let $l = \max\{j_i | 1 \leq i \leq k\}$, then $n_l = N_\infty$.

b) $\to$ **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) $\to$ **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.

□

Definition 1.2.4. A module over a ring R is *Noetherian* iff the equivalent conditions above are fulfilled.

Remark 1.2.2. 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 1.2.2 and the characterization of *Noetherian modules* by Proposition 1.2.3a). For the last assertion, let N and M/N be Noetherian and $X \subseteq M$ be a submodule. Then $X \cap N$ is a submodule of N, thus finitely generated, and $X/(X \cap N) \simeq (X + N)/N$ is isomorphic to a submodule of M/N, thus finitely generated and X is finitely generated by Proposition 1.2.2. □

Remark 1.2.3. Any Noetherian module is finitely generated.

Proposition 1.2.4. *For a ring R the following conditions are equivalent:*

a) R is Noetherian in the sense of definition 1.1.3.

b) R is Noetherian as R-module.

c) Any finitely generated R-module is Noetherian.

Proof. **a**) $\leftrightarrow$ **b**) Follows from the definition.

c) $\rightarrow$ **b**) Obvious, as R is a finitely generated R-module.

b) $\rightarrow$ **c**) Induction on the number of generators of M. Let M be generated by $m_1, \ldots, m_k$ as an R-module and let R-modules generated by $< k$ elements be Noetherian, let $N = \sum_{i=1}^{k-1} R \cdot m_i = \left\{\sum_{i=1}^{k-1} \rho_i \cdot m_i | \rho_i \in R\right\}$ be the submodule generated by the first $k-1$ of the m_i. By the induction hypothesis, is is Noetherian. The map $R \longrightarrow M/N$ sending $r \in R$ to the image of $r \cdot m_k$ in M/N is surjective. This, M/N is isomorphic to a quotient of R, the Noetherian by Remark 1.2.2. Also by Remark 1.2.2, M is Noetherian.

□

Definition 1.2.5. For a module M over a ring R, let $\operatorname{Ann}(M)$ be $\{r \in R \mid r \cdot M = \{0\}\} = \{r \in R \mid r \cdot m = 0 \forall m \in M\}$. It is called the *annihilator* or *annulator* (?) of M.

Proposition 1.2.5. *A module M over a ring R is Noetherian iff it is finitely generated and $R/\operatorname{Ann}(M)$ 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 as an R-module (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 $\{a_n | \sum_{i=0}^{n} a_i T^i \in I, \text{ for some } a_0, \ldots, a_{n-1} \in R\}$. This is an ideal ($R$-submodule) of R, being the image of $I_{\leq n} \longrightarrow R$ sending $\sum_{i=0}^{n} \in I_{\leq n}$ 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 terminates at some $k \in \mathbb{N}$ with $I_n = I_k$ for $n \geq k$. Let $f_1, \ldots, f_A$ be generators of $I_{\leq k}$ as an R-module. We claim that they generate I as a $R[T]$-module. Since they generate $I_{\leq k}$ as an R-module, their k-th coefficients $f_{i,k}$, $1 \leq i \leq A$, generate $I_n = I_k$, for $n \geq k$, as an R-module.

We show, by induction on n, that any $g \in I_{\leq n}$ belongs to $\langle f_1, \ldots, f_A \rangle_{R[T]}$, establishing $I = \langle f_1, \ldots, f_A \rangle_{R[T]}$. For $n \leq k$ we have $g \in I_{\leq k}$ and the assertion is obvious. Let $n > k$ let the assertion be valid for all $\tilde{g} \in I_{\leq n-1}$. Let $g = \sum_{i=1}^{n} g_i T^i$, $g_n = \sum_{i=1}^{A} \gamma_i f_{i,k}$, let $\tilde{g} = g - \sum_{i=1}^{A} \gamma_i T^{n-k} f_i$, then $\tilde{g} \in I_{\leq n}$ as the coefficients cancel. Thus, $\tilde{g} = \sum_{i=1}^{A} \rho_i f_i$ with $\rho_i \in R[T]$ by the induction assumption and $g = \sum_{i=1}^{A} (\gamma_i T^{n-k} + \rho_i) f_i = \langle f_1, \ldots, f_A \rangle_{R[T]}$ as claimed.

Thus I is finitely $R[T]$-generated. Since this holds for any $I \subseteq R[T]$, $R[T]$ is Noetherian. □

Corollary 1.3.1. *As $R[X_1, \ldots, X_{n+1}] \simeq (R[X_1, \ldots, X_n])[X_{n+1}]$, it follows by induction that arbitrary finite polynomial rings over Noetherian rings are Noetherian.*

1.4 Finiteness properties of R-algebras

Definition 1.4.1. Let R be a ring. An *R-algebra* is a ring A (commutative, with 1) together with a ring homomorphism $R \xrightarrow{\alpha} A$. The A becomes an R-module by $r \cdot a := \alpha(r) \cdot a$. 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 1.4.1. If A is an R-algebra and $f_1, \ldots, f_k \in A$, the following subsets of A coincide:

- $\left\{\sum_{d\in\mathbb{N}^k} r_d f_1^{d_1} \cdot \ldots \cdot f_k^{d_k} \middle| r_d \in R, r_d \neq 0 \text{ only for finitely many } d\right\}$
- The image of the ring homomorphism $R[X_1, \ldots, X_k] \longrightarrow A$ 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 1.4.2. 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 1.4.1. *Let R be a ring, A an R-algebra. Any A-algebra B becomes an R-algebra by composition for the homomorphisms.*

a) If A is finite over R, it is of finite type over R. ✓ (trivial)

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

c) If B over A and A over R are of finite type, then B is of finite type over R.

d) An algebra of finite type over a Noetherian ring is a Noetherian ring.

Proof. a) trivial

b) If $(b_i)_{i=1}^m$ generate B as an A-module and $(a_j)_{j=1}^n$ generate A as an R-module, the $\beta_{i,j} = a_j \cdot b_i$ generate B as an R-module: 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 $b = \sum_{i=1}^m \sum_{j=1}^n r_{i,j}\beta_{i,j}$.

c) Let $(b_i)_{i=1}^m$ generate B as an A-module and $(a_j)_{j=1}^n$ generate A as an R-module, then B is generated by $(a_1, \ldots, a_n, b_1, \ldots, b_m)$ as an R-algebra. Let $\beta \in B$, then $\beta = P(b_1, \ldots, b_m) = \sum_{\alpha\in\mathbb{N}^m} p_\alpha b_1^{\alpha_1} \cdot \ldots \cdot b_m^{\alpha_m}$ with $p_\alpha \in A$ which can be written $p_\alpha = q_\alpha(a_1, \ldots, a_n)$ with $q_\alpha \in R[X_1, \ldots, X_n]$, $q_\alpha = \sum_{\gamma\in\mathbb{N}^n} q_{\alpha,\beta} a_1^{\gamma_1} \cdot \ldots \cdot a_n^{\gamma_n}$. Let

$$r(X_1, \ldots, X_m, Y_1, \ldots, Y_n) = \sum_{(\alpha,\gamma)\in\mathbb{N}^{m+n}} q_{\alpha,\gamma} X_1^{\alpha_1} \cdot \ldots \cdot X_m^{\alpha_m} \cdot Y_1^{\gamma_1} \cdot \ldots \cdot Y_n^{\gamma_n},$$

then $R(b_1, \ldots, b_m, a_1, \ldots, a_n) = \beta$ establishing our claim that $\{a_j\} \cup \{b_i\}$ generate B as an R-algebra.

d) 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 1.4.2 (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 $(a_i)_{i=1}^n$ generate A as an R-algebra and let $(\alpha_j)_{j=1}^n$ generate it as a B-module. We have expressions

$$a_i = \sum_{j=1}^{n} b_{i,j}\alpha_j \tag{1}$$

$$\alpha_k \cdot \alpha_k = \sum_{j=1}^{n} \beta_{j,k,l}\alpha_j. \tag{2}$$

Let $\tilde{B} \subseteq B$ 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 $\tilde{A} \subseteq A$ be the $\tilde{B}$-submodule generated by the $(\alpha_k)_{k=1}^n$. It is a subring by (2) and contains the a_i by (1) and is an R-algebra because $\tilde{B}$ is. Then $\tilde{A} = A$ and A is finite over $\tilde{B}$. Since $\tilde{B}$ is Noetherian and $B \subseteq A$ is a $\tilde{B}$-subalgebra and B is finitely generated as $\tilde{B}$-module ($\tilde{B}$ being Noetherian), hence B is of finite type over $\tilde{B}$ (Proposition 1.4.1a), hence B is of finite type over R (Proposition 1.4.1c) □

Proposition 1.4.3 (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 1.4.3. See Matsumura, CRT, for Eakin-Nagata.

1.5 The notion of integrity and the Noether Normalisation Theorem

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

Definition 1.5.1. Let $A \subseteq B$ be a ring extension. We call $b \in B$ integral/ganz over A if it satisfies an equations

$$b^n + \sum_{i=0}^{n-1} a_k b^k = 0$$

with $a_k \in A$. We call B over A integral, if every element of B is integral.

Remark 1.5.1. It is not really necessary to assume $A \to B$ to be injective.

Proposition 1.5.1. *a) $b \in B$ 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 elements of B which are integral over A, the there is an A-subalgebra $A \subseteq C \subseteq B$ which is finite over A and containing all b_i.*

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

c) If C/B and B/A are integral, C/A is integral.

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

Proof. a) Let $b_1, \ldots, b_n$ be integral over A and let C be the subring generated over A by $b_1^{\alpha_1} \cdot \ldots \cdot b_n^{\alpha_n}$ with $\alpha \in \mathbb{N}^n$. Each b_i satisfies an equation $b_i^{D_i} = \sum_{j=0}^{D_i - 1} a_{i,j} \cdot b_i^j$ with $a_{i,j} \in A$. Then it follows by induction on k that b_i^k is an A-linear combination of b_i^j with $0 \leq j < D_i$. If follows that C is generated as an A-module by $\{\prod_{i=1}^n b_i^{e_i} | 0 \leq e_i < D_i\}$ and C is as desired. This the second assertion of *a*), which contains one direction of the first as a special case. For the other direction let $C \subseteq B$ be an A-subalgebra which is finitely generated, e.g. by $(\gamma_i)_{i=1}^n$, as an A-module. Let $b \in C$, $b\gamma_i = \sum_{i=1}^n m_{j,i}\gamma_j$ with $m_{j,i} \in A$. The matrix $M = (m_{i,j})_{i=1}^n {}_{j=1}^n$ satisfies its own characteristic equation by Cayley-Hamilton: $M^n = \sum_{i=0}^{n-1} p_i M^i$ with $p_i \in A$. Since b^j in C can be expressed by (in the sense hat [insert diagramm here]) it follows, that $b^n \cdot c = \sum_{i=0}^{n-1} p_i b^i c$ (first for $c = \gamma_i$, then all of C). Taking $c = 1$ shows $b^n = \sum_{i=0}^{n-1} p_i b^i$ as stated.

b) 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.

c) Let, more generally, B/A be integral and $c \in C$ integral over B. It satisfies an equation $c^d = \sum_{i=0}^{d-1} \beta_i c^i$ with $\beta_i \in B$. By a), there is an A-subalgebra $\tilde{B} \subseteq B$ which is finite over A and contains the β_i. Then c is integral over $\tilde{B}$, hence by a) there is a $\tilde{B}$-subalgebra $\tilde{C} \subseteq C$ containing c and finite over $\tilde{B}$. Now $\tilde{C}/A$ is finite by Proposition 1.4.1b), hence c is integral over A by a).

□